
LOOKING AHEAD: PREPARING FOR
INFORMATION-AGE CONFLICT

John Arquilla and David Ronfeldt

As we assembled this volume, we initially expected to conclude it in a standard manner: revisiting themes noted in the introduction, summarizing key points from the selections, and identifying issues for future research and development. This concluding chapter still has some of that flavor. But as we discussed how to write it, we realized our thoughts were cohering around four sets of ideas which, together, amount to the outlines of an integrated vision of information-age conflict—from how to think about it, to how to prepare for it and deal with it.

As a result, this chapter represents not only the conclusion of this book but also the beginning of an integrated vision of information-age conflict. This vision has four parts—conceptual, organizational, doctrinal, and strategic. Each part of this vision is tied to the others; each energizes the others.

- **Conceptual foundation:** This vision entails, indeed requires, a deep, broad view of “information.” This is achieved by adding to the dominant view that information is largely about “information processing” a less-developed view that is about “information structuring” or “structural information.” In this latter view, information is what enables a structure to hold its form. This broad view of information refocuses thinking about the significance of information to organizations and leads to a recognition that their ideational superstructures are as important as their technological infrastructures.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 1997		2. REPORT TYPE		3. DATES COVERED 00-00-1997 to 00-00-1997	
4. TITLE AND SUBTITLE Looking Ahead: Preparing for Information-Age Conflict				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School, Graduate School of Operational and Information Sciences, Department of Defense Analysis, Monterey, CA, 93943				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES In Athena's Camp: Preparing for Conflict in the Information Age (John Arquilla and David Ronfeldt eds.) Santa Monica, CA: RAND, 1997					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 63	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

- **Organization:** This vision emphasizes adapting to a major consequence of the information revolution—the rise of network forms of organization. The information revolution is empowering small forces and formations that can best take advantage of the network form. Some actors, such as transnational terrorists and criminals, are moving to networked designs. For governments and militaries, the challenge will be to develop hybrids in which “all-channel” networks are fitted to flattened hierarchies. The major benefits may accrue in the areas of interagency and inter-service cooperation. Since militaries must retain hierarchical command structures at their core, their hybrids should retain—yet flatten—the residual hierarchy, while allowing dispersed maneuver “nodes” to have direct, all-channel contact with each other, and with the higher command.
- **Doctrine:** An integrated vision in this area should extend across the spectrum of conflict from low to high intensity, and across all services and other agencies. Our vision holds that “swarming” may be the key mode of conflict in the information age—it is more feasible than ever for offense and defense, across the entire spectrum of conflict. To develop advantages from the dynamics of networking among small, dispersed forces, a new doctrine, and related strategies and tactics, should be developed around swarming, whose full implications may mean that AirLand Battle should be superseded by a “BattleSwarm” doctrine.
- **Strategy:** Making this vision work depends on achieving unprecedented levels of information sharing—be that at the tactical level to enable small forces to cohere and swarm as networks in wartime, or at the level of grand strategy to advance U.S. power and influence around the world in peacetime. But U.S. interests also require that information sharing be protected. The development of a strategy of “guarded openness” is advisable at all levels, including at the level of grand strategy. We propose that a “revolution in diplomatic affairs” (RDA) be undertaken to match the revolution in military affairs (RMA) now under way.

Of course, information has always mattered; networking has long characterized some organizations; swarming has a history, especially in irregular warfare; and guarded openness is a traditional posture for democracies. What is new is the vastly increased degree to which

each part of this vision matters now, and the increased degree to which the parts are interwoven.

We hope this vision proves useful for thinking about and preparing for conflicts and other interactions in the coming years. But we acknowledge that our ideas remain formative. We state them firmly, with studied conviction, but we know that more thought, research, and analysis must occur before definite answers and solutions emerge. This applies to all parts of our vision; each may develop in an uneven, perhaps ragged, fashion. Heeding the counsel of Stephen Rosen (1991, pp. 243–262), we mean to present our ideas not as though they amount to the “single best route to innovation,” but rather as a road map, one of many that may merit exploration and elaboration, for helping come up with a broad, flexible “strategy for managing uncertainty” in a time of flux.

TOWARD A MORE STRUCTURAL VIEW OF INFORMATION

Lately, “information” has become an elusive concept, difficult to define. The more the information age deepens, the more this is evident. Questioning and rethinking are continually called for.

How a concept is defined affects what people think is most important. In most discourse, the term “information” is, and really can be, used without much questioning, largely because substantial traditions have grown around its usage. Thus, as an earlier study observed (see Chapter Six), information is normally regarded as being about a “message” and/or a “medium.” Meanwhile, that paper noted, a speculative new idea is emerging that views some information as being “material”—as lying grandly at the core of all existence, where it may be as fundamental as matter and energy.¹ This is a heady, challenging idea that continues to gain ground; George Johnson’s *Fire in the Mind* (1995) offers a good overview of the idea, much of which falls under the rubric of “information physics.”

We draw on further ruminations and readings to look at information under two overarching views. One dominant overarching view is the “information processing view.” We propose that it be balanced by another overarching view, a “structural information view,” which has not yet received much articulation. And we identify some implications—indeed, clarifications—that this rebalancing may offer.

Information Processing and Structural Information Views

The view that “information” is mostly about signals being transmitted between senders and receivers—that is, about messages and the media through which they get communicated—is often summed up as the “information-processing view.” It stems from the work of the seminal information theorists Claude Shannon, Warren Weaver, and Norbert Wiener in the 1940s; and for most contemporary theorists, it is the dominant view about information, including about its effects and implications for organizations and societies. James Beniger’s *The Control Revolution* (1986, pp. 9–10) offers an exemplary picture of this view, in which “information processing is essential to all purposive activity”:

Information processing may be more difficult to appreciate than matter or energy processing because information is epiphenomenal: it derives from the organization of the material world on which it is wholly dependent for its existence. Despite being in this way higher order or derivative of matter and energy, information is no less critical to society. All living systems must process matter and energy to maintain themselves counter to entropy, the universal tendency of organization toward breakdown and randomization. Because control is necessary for such processing, and information, as we have seen, is essential to control, both information processing and communication, insofar as they distinguish living systems from the inorganic universe, might be said to define life itself—except for a few recent artifacts of our own species.

In recent years, expansive versions of this view have extended to claims that all physical matter (not to mention energy) as well as all biological and social systems have information at their core, and moreover that their motion, behavior, and evolution all revolve around information-processing (e.g., see Haefner, 1992; Johnson, 1995).² The grandest claims urge that the universe is tantamount to a giant computer or cellular automaton. In short, “everything is information.”

But while much information is about processing, and while the processing view offers much that is systematic and sensible, there comes a point at which “processing” seems inadequate, inaccurate, or at least insufficient, both as a scientific concept and as a meaningful metaphor, for getting at what information is all about. One ends up

with a series of processes piled on other processes. Information is not seen to have significance if it has no bearing as a message or message modifier in a process. It is seen as something that enters or exits a structure, or exists within it, primarily for the purpose of receiving, processing, and/or sending other information, matter, or energy on its way.

Yet much information may just be residing somewhere, embedded, doing little or nothing in the way of processing, while doing a lot to define a particular structure, give it shape, and hold it together—be it a physical, biological, or social structure. Such information is engaged less in “processing” than in “structuring.” We do not introduce this point to deny the validity of the processing view, but rather to propose that a structural view—call it an “information structuring” or a “structural information” view—can add to our understanding of information and reorient thinking about it in useful ways.

Indeed, efforts to spell out the processing view eventually make statements about structure. According to one book, for example, information processing systems depend on the “internal information” that is a constitutive and “necessary component of every natural structure” and that allows external information “to be processed appropriately” (Haefner, 1992, pp. 4, 45). Moreover, “structural information” and “embodied knowledge” are essential parts of all information processing systems (Oeser, 1992, pp. 325–326). Such remarks start to elevate structure. Would it not be advisable to take steps to distinguish structure from process, and to place them on more equal analytic footings?

Structure and process are different—and in most sciences both are deemed essential for characterizing any system and its workings. Theorists in the physical and the social sciences tend to emphasize structural views—in “the structure of the atom” and “the structure of society.” In contrast, “life processes” tend to get emphasized in the biological sciences. But whether structure or process is emphasized, neither is neglected—social theorists also study “the democratic process” and “the process of modernization,” and biologists “the structure of the body.” Indeed, theorists often bounce back and forth between issues of structure and process (sometimes by other names).

Explicit statements about the importance of including both structure and process are not common in the literatures of these varied sciences; theorists who study systems often use the terms without providing adequate definitions of either. But when such statements occur, the writers are often quite emphatic, as the following excerpt illustrates:

The fact is that there are two traditions of explanation that march side by side in the ascent of man. One is the analysis of the physical structure of the world. The other is the study of the processes of life: their delicacy, their diversity, the wavering cycles from life to death in the individual and the species. And these traditions do not come together until the theory of evolution . . . (Bronowski, 1973, p. 291).

In social and political theories, focusing on “structure” generally means focusing on actors (and “objects”) and the organization of their relationships to each other (e.g., hierarchical relationships). Focusing on “process” generally means focusing on interactions and their dynamics. Structures contain the actors, processes the interactions; and both structure and process must be joined in systems theory (e.g., Bertalanffy, 1968; Waltz, 1979).³ In many accounts, structure outweighs process—or at least it gets the dominant attention (e.g., Skocpol, 1979).⁴ But in other accounts, copious processes prevail, because they may create new structures (e.g., Lenski, 1966).⁵ In any case, the boundaries between structure and process are rarely sharply defined. Moreover, spirals of cause and effect involve both, inextricably. In short, both are important for understanding systems, and if one is discussed without the other, something is missing.

What does this have to do with information? Writing about information has long focused on notions about process, rarely about structure. Thinking about the concept of information, and about how a concept may have practical implications, will benefit from building up a structural view, as both a complement and a supplement to the processing view. We have not found any eminent guidance as to what a structural view of information should look like; but a working start might go like this: All structures contain embedded information. Where there is structure—or pattern or organization—there is information. Somehow, the amount of structure and the amount of information go together. Embedded information is what enables a structure—be it physical, biological, or social—to hold its form, to

remain coherent, even to evolve and adapt. All forms of organization thus depend on embedded information; they do not have shape, and cannot retain their shape, without it. Indeed, the fact that incoming information may get restructured before it is absorbed, processed, and/or sent on its way may testify to the depth of the embedded information—it corresponds to a kind of cultural bias built into the structure, defining its identity and setting its predispositions. This is not to say that “everything is information” but rather that “everything has information” embedded in it if it has structure.

Few past efforts have gone in this direction. In one keen effort, though, Robert Wright (1989, p. 94) verges on adopting a structural view when he writes about how to define information:

Apparently, information not only has structure; it is a prerequisite for the creation of structure—and for its preservation. It doesn’t merely embody order; it advances order and maintains it. Information lies not just in form; information lies in formation. It is the stuff that leads the fight against the second law [of thermodynamics].

Unfortunately, he quickly abandons this view because it does not live up to what he thinks is needed for a definition of “real-life information,” and his search for such a definition in the rest of his book is driven mainly by processing concerns.⁶ But at least he illuminates a path not taken.

In this light, consider a map, any map: Does it process or structure information? Actually, it does both—and to assert that it is just one or the other is to miss half the full truth. The map serves as an information processor when the reader uses it to tell where he or she is. At the same time, the map as a whole portrays information about the structure of a territorial expanse.⁷ Consider the written word: Is it for processing or structuring information? It is used for communication, which in most views is a kind of processing. Yet, a written language is based on agreements that particular assemblages of scribbled shapes have distinct meanings—what the message and the medium convey stems from deep symbolic and material structures, as well as processes, within a society. Consider a business or other organization: Is it better to view it as an information processor or structurer? Again, the best answer is “both”—although it is a more common practice these days to see an organization as a processor.

The general point, then, is not that the processing view is wrong but that, in one context after another, it is insufficient and, by itself, risks overextension if it is made the sole lens for looking at the role of information in organizations. A framework that also includes a structural view should be stronger analytically and should reveal "information" to be an even deeper, broader concept than often thought. Adding a structural view and keeping it in balance with the processing view may also have interesting, reorienting effects on the practical implications that a theoretical concept of information may lead to. Adding a structural view may help compensate for some biases that occasionally creep into the processing view (but may lead to new biases if too much weight is given to the structural view alone).

The processing view puts the spotlight on the transmission of messages, often as the inputs and outputs of a system. It lends itself to computational approaches that focus on data processing. It tends to emphasize the importance of the technological infrastructure. In so doing, it leads to thinking that organizations can be enhanced by adding new information and communications technologies, without necessarily having to change the organization's structure in order to adapt advantageously to a technology. Such biases are not always the case—the point that technology alone cannot improve an organization is well known to many expert exponents of the processing view—but they are common. Moreover, where an organization is resistant to change, an emphasis on the processing view may make it more likely that both the proponents and opponents of change shy away from posing and confronting structural questions about the nature of the organization.

In contrast, a structural view casts a spotlight on the values, goals, and principles that an organization embodies—on what matters to it and to its members, from the standpoint of its identity, meaning, and purpose as an entity, apart from whether it is doing information processing. A structural view relates to that part of the information revolution that is said to be about "knowledge"—it cannot be about "data," since data do not determine the nature of a structure. A structural view underscores how much a vibrant organization depends on deeply embedded information, and how difficult and complex it may be to change an organization. The best of the processing views may understand this as well; but it is not their normal

starting point, which tends to be more about efficiency than about meaning and purpose. A structural view assumes at the start that an organization's information infrastructure is only part of the picture; more important is its ideational superstructure (see below). While the processing view tends to illuminate technology as a critical factor, a structural view is more likely to uphold human capital. While the processing view seems to appreciate quantitative approaches to information, a structural view is likely to be more qualitative.

We are not alone in espousing this perspective.⁸ It has much in common with one espoused recently by the Japanese knowledge theorists Ikujiro Nonaka and Hirotaka Takeuchi (1995). Their criticisms of the information processing view are similar to ours. More to the point, their proposals for a broad new view that emphasizes "tacit" knowledge (which is largely qualitative and cultural, and different from "explicit" knowledge) are akin to our ideas about structural information:

Although Western managers have been more accustomed to dealing with explicit knowledge, the recognition of tacit knowledge and its importance has a number of crucially relevant implications. First, it gives rise to a whole different view of the organization—not as a machine for processing information but as a living organism. Within this context, sharing an understanding of what the company stands for, where it is going, what kind of a world it wants to live in, and how to make that world a reality becomes much more crucial than processing objective information. Highly subjective insights, intuitions, and hunches are an integral part of knowledge. Knowledge also embraces ideals, values, and emotion as well as images and symbols. These soft and qualitative elements are crucial to an understanding of the Japanese view of knowledge (Nonaka and Takeuchi, 1995, p. 9).

It is encouraging for us to find that other thinkers are moving in this vein. Yet, while Nonaka and Takeuchi pinpoint how Western and Japanese management views may differ, the challenge for the United States will be to formulate views that have global, as well as national, appeal.

Infrastructure and Superstructure Are Both Important

Some of these points may be visualized, and summed up, by taking a new look at the “information pyramid”—the distinction between the structural and the processing views casts a new light on it. As discussed in an earlier paper (see Chapter Six), the pyramid, recast in Figure 19.1, has a wide base of raw, disorganized “data” and “facts,” atop which sits a narrower stratum of organized “information.” The next, still narrower stratum corresponds to information refined into “knowledge” (including “ideas”). Atop that, at the peak, sits the most distilled stratum, “wisdom”—the highest level of information. The pyramid may appear to imply that the higher levels rest on the lower, but that is true only to a degree. Each layer has some independence—more data does not necessarily mean more knowledge, and as critic Theodore Roszak (1986) objects, in a wide-ranging attack on the information processing view, “information” should not be mistaken for “ideas.”⁹

The processing and structural views can be identified with different strata in this pyramid, as indicated in Figure 19.1. The processing view relates mainly to the lower two strata. Its articulators write

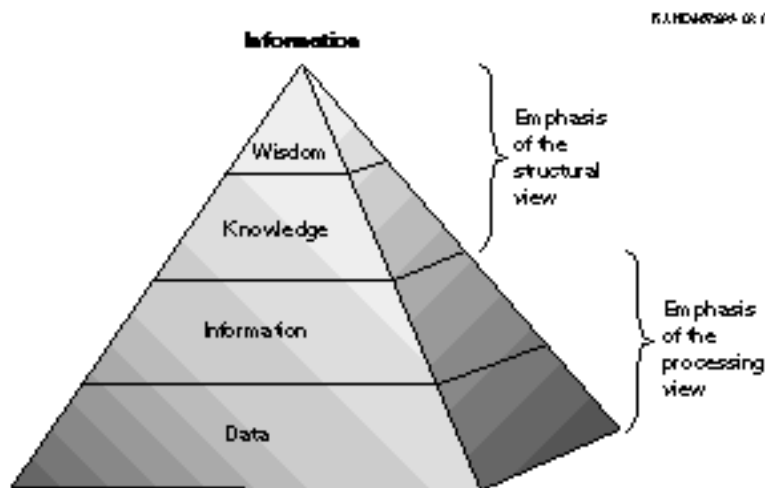


Figure 19.1—The “Information Pyramid” from Two Views

mainly about the processing of data and information; they rarely discuss knowledge processing,¹⁰ and normally shy away from notions of wisdom processing. In contrast, the structural view shifts the focus. It is very much about the top two strata—it relates to the laws, rules, strictures, codes, goals, ideals, and values that are embedded and embodied in institutions, cultures, and other structures. The lowly data stratum may have little or no significance for a structuralist.

Can we be more specific about what a “structural information view” may look like analytically? Insofar as societal structures are the focus—and that is our key concern here, not physical and biological structures—we will borrow from the social science literature to propose that a structural view could include (or be decomposed into) the following levels or layers: an ideational superstructure, an organizational structure, a technological infrastructure, and possibly also a linguistic substructure.¹¹

- The “ideational superstructure” is the level of ideas and ideologies, myths and maxims, values and norms, rites and rituals, laws¹² and rules, etc. that define, often abstractly, the nature of a culture and the structures within it. A structural view should, among other things, lead the analyst’s eye to the belief systems in a society about information and communications—about what it may mean to have an “information culture,” be part of the “information revolution,” and develop an “information society.” Debates about whether a particular government should allow people to own computers and connect to the Internet may pertain here, particularly if those debates reflect broader beliefs about the nature of a society.
- The “organizational structure” is the level of particular organizations in a society. Broadly speaking, the structural view holds that all organizations depend on information and may be analyzed as information structures. Narrowly speaking, this is the level for identifying which organizations in a society (and still more narrowly, which offices in a corporation or other entity) are concerned with information and communications matters specifically. Societies differ greatly according to the richness, or the lack, of organizations for dealing with such matters: Are they concentrated in the government sector? Or the market sector? What about civil society? As to the last, it is noteworthy that very

few societies have entities like the Electronic Freedom Foundation (EFF) or Computer Professionals for Social Responsibility (CPSR).

- The level of the “technological infrastructure” refers to all the hardware and software systems, and all the connectivity, that support communications and information flows—not simply the Internet, but television, radio, telephones, etc.¹³ This is, of course, the level that the information-processing view tends to focus on.¹⁴
- Though debatable, it may be wise to posit a “linguistic substructure” as a distinct level—this would recognize that much of what may emerge and take shape at the other levels, and especially at the ideational level, may depend on linguistics, or perhaps it would be better to say the cognitive and epistemological orientations of a society. This is the level where the most basic concepts are formed about what matters and what is possible. For example, this is the structural level where it may make a difference whether English or some other language dominates discourse on the Internet or in television satellite broadcasts.

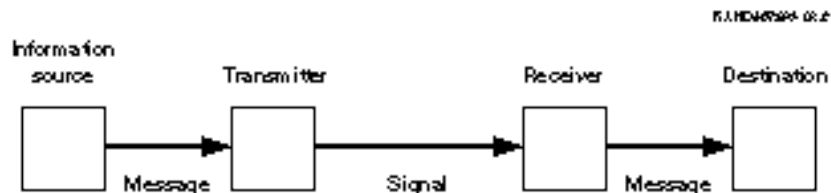
At all these levels, information remains central to the analysis of order and change in systems, but in ways different from the case with the processing view. Ideally, there should be “coherence” within and among all levels; “information decoherence” (term from Johnson, 1995) may bring on structural instability, leading possibly to breakdown and/or radical reform. Indeed, in this view, conflicts occur because of differences in structural information (e.g., in religious beliefs at the ideational level), more so than because of differences in information processing capabilities. The structural view, like the processing view, may be used for comparing societies—but with the advantage of encouraging analysis that goes well beyond technological factors.

Figures 19.2 and 19.3 portray the two views. Figure 19.2 shows an input-output diagram of an information processing system in which a sender transmits a message to a receiver by way of a channel. The structural view requires a different diagram. Figure 19.3 depicts the information-related structures noted above—an organizational structure bound with an ideational superstructure and a technological infrastructure, and also having a cognitive/linguistic substructure

at its core. This diagram is not about inputs and outputs but rather about interrelationships, as signified by the up-down arrow.

Developing a structural view to blend with the processing view could lead to the fusion of separate traditions in “communication studies” and “information theory”—and this fusion could benefit policymakers and strategists who are trying to figure out what “information strategy” America should follow today. As noted earlier, discussions based on information theory hark back to the work by Shannon and others in the 1940s and 1950s that gave rise to today’s technology-oriented view of information. Indeed, Figure 19.2 modifies a diagram by Shannon, a founding father of information theory. But while “information” was receiving the kind of attention at mid-century that stressed its engineering dimensions, “communication” was receiving another kind of attention among another set of theorists who emphasized the ideational dimensions.

Everett Rogers (1994, pp. 10–16) shows that the field of communication studies developed in the 1930s and 1940s was dominated by such leading social scientists as Harold Lasswell, Paul Lazarsfeld, and Wilbur Schramm. While they were broadly interested in communications issues, World War II drove them to focus intently on understanding propaganda, measuring public opinion, analyzing the impact of the media, and using communications to influence public



NOTE: This is a variant of a famous diagram by Claude Shannon and Warren Weaver. In particular, our variant omits the introduction of “noise” that may mean the signal sent is not the signal received. If we were to leave noise in this figure, we would have to add it to Figure 19.3—but that could raise a whole new issue for discussion that is better left to future elaborations of our present ideas.

Figure 19.2—Classic Information-Processing View

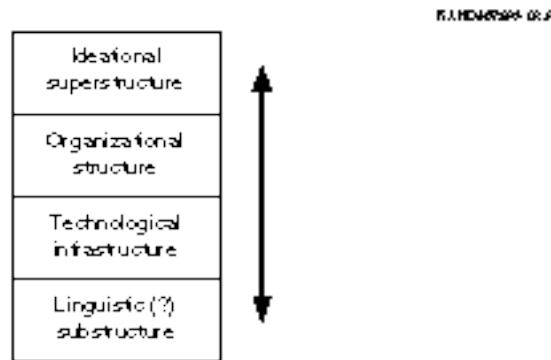
**Figure 19.3**

Figure 19.3—An Information Structuring View

and private behavior on behalf of the war effort (e.g., to promote the cultivation of “victory gardens”). While these social scientists gave some attention to developments abroad (e.g., to support “black propaganda”), their primary focus was defending and strengthening public morale on the home front. The guiding phrase for research came from Lasswell in 1940: “Who says what, to whom via what channels, with what effects?” But the most prescient warning for policy and strategy was sounded by Schramm shortly after Pearl Harbor: “Perhaps more than any previous war this is likely to be a war of communications.”

In short, the rise of information theory depended on hard scientists, and that of communication studies on social scientists. While the work of the information theorists went into improving America’s weapons systems, that of the communication experts went into protecting our value systems. While the ideas of the information theorists moved in the direction of cybernetics and general systems theory, those of the communication experts led to new schools and centers for elevating the study of public opinion, the media, and journalism.

Today, it is advisable for information strategists to develop a structural view to go with the processing view. The latter view undergirds

current notions that analysts and policymakers should focus on the information technology infrastructure—and, from an information-warfare perspective, on the vulnerabilities of that infrastructure to attack. But this bias neglects the importance of the ideational superstructure—and the prospect that an information-warfare attacker may want the technology (e.g., the Net) working so that public or elite opinion can be influenced, whether by single, perhaps frightening moves, or through multiple nuanced measures that may have cumulative corrosive effects. In key respects, the history of communication studies is more about structural information, especially at the ideational level, and about protecting it from the kinds of attacks that technologists have not been attending to. This history serves to substantiate that today's information strategists should be adopting a broader view than has been purveyed by many information-warfare scenarists.¹⁵

Both traditions also speak to the importance of U.S. government and foundation sponsorship for innovative research. With the arrival of World War II, the fields of information theory (including cybernetics) and communication studies were given separate impetus through support provided by U.S. government (especially military) offices that not only sponsored research but also worked to create networks for sharing knowledge between government and academic researchers. For example, the Office of Facts and Figures (OFF), later the Office of War Information (OWI), and, apart from it, the Rockefeller Foundation (through the Rockefeller Communication Seminar) played key roles in the shaping of communication studies. Today, a key government role is played by a set of offices in the Pentagon, particularly in the Office of the Secretary of Defense (Command, Control, Communications, and Intelligence), which is continuing this tradition.

Building Bridges to Organization, Doctrine, and Strategy— and More

This is a preliminary basis for formulating a structural view and matching it, in a balanced way, to the processing view. Yet, working with these two overarching views seems to offer a better basis for creating a conceptual framework about information than did our earlier tripartite distinctions about the message, the medium, and

the material view of information. That earlier approach is engulfed by the one presented here.

For example, a structural view appears to deepen understanding of the human and the technological factors at stake. Regarding the human factors, education and training programs obviously serve to improve the knowledge base of an organization. But the ways that information gets imparted and embedded may run deeper than explicit education. Consider the practice of daily routine marching and drilling, which was instituted by the Dutch and French armies in the 17th century (although the Roman army had set some precedents). William McNeill (1982, pp. 125–132) relates that this simple practice had unexpectedly profound psychological and cultural effects that made soldiers more efficient and effective. Through routine drill, soldiers became more prone to obey orders from their commanders, to bond socially with others in their unit, to gain a sense of *esprit de corps* even though they came from different villages and strata, and to feel separate from people in society at large. Meanwhile, they also gained knowledge about how use new weapons on the battlefield. Marching and drilling are not normally viewed as ways to embed tacit information in a fighting force—and that is why we raise it here. It materially strengthens the unit, in part by strengthening the immaterial dimensions of power: will power, discipline, and camaraderie. This is the case, as well, with later, more advanced, explicit types of training, education, exercise, and simulation.

As to technology, a structural view clarifies further what we meant earlier (see Chapter Six) by the “information package” of a weapon. That term (or alternatives, like “information quotient”) refers not just to the processing systems associated with the weapon (e.g., for guidance) but to the whole set of technologies embedded structurally in it. The information revolution may make ideas more valuable than things—but a structural view implies that the distinction between “ideas” and “things” is blurring, particularly as things may be viewed as the embodiment of ideas.

The larger question for this study is: Does the addition of a structural view help with our effort to convey the organizational, doctrinal, and strategy parts of an integrated vision? We think so, and we will point out how as we discuss these parts in the pages that follow. Perhaps more than anything, the addition of a structural view illuminates

how complex innovation can be, and how very difficult it can be to try to institute radical organizational, doctrinal, and strategic changes.

ADAPTATION TO NETWORKED FORMS OF ORGANIZATION

The information age is facilitating two major organizational trends: one is the rising power of small groups, the other is the rise of network forms of organization. The two trends feed on each other—networks of small actors stand to gain more power and influence than they have previously ever had.

Thus, the organizational part of our effort to posit an integrated vision of conflict in the information age reiterates a theme we have long emphasized: the rise of network forms of organization (Arquilla and Ronfeldt, 1993, 1996; Ronfeldt, 1992, 1996). The basic argument is that the information revolution favors the rise of networks, while making life difficult for hierarchies. The type of network especially favored is the “all-channel” type, in which diverse, dispersed, often small actors (or “nodes”) all link together to consult, coordinate, and act jointly, preferably in a non-hierarchical manner, across greater distances and on the basis of better and faster information than ever before. Network designs have been in existence since ancient times, but new information technologies finally provide for the abundance of information connections and flows that network designs require.

The rise of network forms of organization remains at an early stage, still gaining impetus. It may be decades before this trend reaches maturity. But it is already affecting all realms of society in positive ways. For example, in the realm of the state, it is facilitating the formation of interagency mechanisms for addressing complex policy issues that cut across jurisdictional boundaries. In the realm of the market, it has been facilitating the emergence of Japanese keiretsus and similar distributed, web-like global enterprises (including “virtual corporations”). Indeed, volumes are being written, mostly in the United States and Japan, about the benefits of network designs for business corporations and market operations—to the point that casual observers might presume that this is the realm most affected and benefited.

However, although the evidence is still sparse, it appears that civil society actors are heavily favored by the effectiveness of network designs. Nongovernmental organizations (NGOs) that once had to operate largely in isolation from each other can now cluster together. The trend seems keenest among the multi-organizational networks that have been multiplying among relatively small activist NGOs (e.g., those for human rights and environmental issues) across the political spectrum—and across national boundaries. In the long run, civil society is likely to be strengthened more than the other realms. Indeed, for some NGOs the long-range aim is to construct a transnational “global civil society” powerful enough to counterbalance the roles of state and market actors.

Overall, then, the trend toward “the age of networks” is so strong that, projected into the future, it augurs transformations in how societies are organized—if not in societies as a whole, at least key parts of their governments, economies, and especially their civil societies. This all sounds positive. But, meanwhile, the rise of the network form also augurs a new epoch of conflict.

Power is migrating to small, mostly nonstate adversaries who can organize into sprawling networks more readily than can traditionally hierarchical nation-state actors. Not only civil society but also “uncivil society” is benefiting from the rise of network forms of organization. Some uncivil actors, such as terrorists and criminals, are having little difficulty forming highly networked, nonhierarchical organizations. Thus, networked adversaries may be expected to pose increasing threats to the United States and its interests around the world. Conflicts will more often be fought by “networks” than by “hierarchies.”

It will not be easy for hierarchies to fight networks in the information age; to a considerable degree, it will take networks to fight networks. Yet, state actors, such as professional militaries, cannot do without their hierarchies; they must continue to uphold hierarchy at their core. At the same time, they should not forgo the advantages of using network-based designs, particularly to increase their agility and flexibility for field operations. The challenge will be to combine hierarchical and network designs. In our view, the U.S. military and other security actors should aim to adapt hierarchies to networks by synthesizing hybrids.

Networked Adversaries on the Rise

The major motivation for the U.S. government to adapt to network forms of organization comes not from alluring theories about the likely efficiency and effectiveness benefits, but rather from some distressing new realities: Many adversaries of U.S. interests are well along the path of learning to utilize networks to improve their agility and versatility. This is particularly the case with actors at the low-intensity end of the spectrum of conflict and crime.

Uncivil actors—such as terrorist groups and criminal gangs—once operated pretty much in isolation from each other. But now, hierarchical Mafia clans led by “dons” and “capos,” modeled on the Roman empire, are giving way to much “flatter” transnational criminal organizations (TCOs), such as seen among the Colombian and Mexican drug cartels, the Asian triads, and even in Chicago’s Gangsta Disciples. Similarly, terrorist organizations are leaving behind the era of the “great man” leader, and moving to use flexible network designs that may have multiple leaders. The PLO of Arafat is less the paradigm than the “governance of the many” seen in Hamas. Transnational terrorist organizations are emerging on the political left (e.g., Hamas) and on the right (e.g., among “white supremacy” and “skinhead” groups). All are building transnational networks as “force multipliers,” and using all manner of old and new communications technologies to do so. Because of the shift from absolutist hierarchies to hydra-headed networks, none are as easy to “decapitate” as they may once have been.

Besides terrorists and criminals, the low end of the conflict spectrum is also populated by information-age revolutionaries and old-style ethnonationalists. They too seem increasingly comfortable with networked organizational structures, which are commonly enhanced by kinship ties. That these actors have gained strength and flexibility through networking is seen in two recent cases of netwar. First, as related in Chapter Sixteen, the Zapatista insurrection in Chiapas featured a small insurgent force, acting as the striking arm of a local network of Mayan peoples, that was able to build additional, transnational networks with activist NGOs from around the world in a successful effort to constrain the Mexican government from crushing the rebellion bloodily, and instead persuade it to agree to political negotiations. Second, the Chechen struggle against the Russians

shows that a networked rebel force, composed of small bands of 12 to 20 fighters, can confront, and beat, a modern army. This case raises the possibility that networked forces can fight not only insurgencies, but also mid-level, and even quite high-intensity, conflicts.

The rise of a new generation of networked adversaries—terrorists, criminals, insurgents, and ethnic warriors—raises questions about whether today's professional military and police forces and intelligence agencies have the most appropriate organizational structures for an era in which new destructive and disruptive powers are migrating into the hands of small groups that are internetted with other small groups. As Van Creveld (1996, p. 58) remarks,

In today's world, the main threat to many states, including specifically the US, no longer comes from other states. Instead, it comes from small groups and other organizations which are not states. Either we make the necessary changes and face them today, or what is commonly known as the modern world will lose all sense of security and will dwell in perpetual fear.

Endurance of Hierarchies, Advent of Networks

Can modern hierarchies do well against information-age networks? Debates about hierarchies versus networks are filling up bookshelves these days. These debates have two levels, which should not be confused. One level is deep, theoretical, and philosophical. At this level, theorists have been arguing that hierarchies or networks (or markets, for that matter) are the key form of organization, or set of dynamics, that underlies essentially all order (and maybe chaos) in the world. In the social sciences, for example, some early writings about general systems theory (e.g., Bertalanffy, 1968) and complexity (e.g., Simon, 1962) took stances lauding the roles of hierarchies. Today, arguments are coming to the fore that networks are the crucial design, such that "the web of life consists of networks within networks," not hierarchies (Capra, 1996, p. 35). This is an enlightening debate, but it is not the more practical of the two.

The second level of debate is practical and empirical; it has theoretical and philosophical dimensions as well, but they are generally tied to real-life matters in the worlds of government, military, and business affairs. In this debate, hierarchies and networks (not to mention

markets) are distinct, bounded forms of organization that enable people and other societal actors to do practical things. Hierarchies, of one variety or another, are recognized as having lain at the administrative core of states, militaries, and corporations for centuries. Today, networks, especially the all-channel variety, are being touted and examined, sometimes carefully, sometimes with incautious exuberance, as the up-and-coming form of organization for gaining the agility, flexibility, and versatility that a government agency, business enterprise, or civil-society actor may desire for doing well in the information age.

This level of debate is many-faceted. However, here we focus only on two points that are consistent with our central theme for the organizational part of our vision: the advisability of moving toward networked designs. First, hierarchies are not “goners” because of the information age—but they must adapt. Second, learning to blend hierarchies and networks into workable hybrids is essential—but it will not be an easy task.

The dawning of “the age of networks” does not spell the end of hierarchy, or the nation-state, as some thinkers have speculated. Theorists should be wary of such speculations because hierarchies, of one variety and then another, have been eroding and becoming outmoded for centuries, often as a result of epochal shifts in information and communication technologies. The classic, oft-noted example is the decline in the power of that great hierarchy the Papacy, and of the Catholic Church more generally, as a result of the spread of the printing press—but this decline gave way to the rise of monarchies and then nation-states as powerful new hierarchies (Anderson, 1991; Anderson, 1974). Later, during the period from 1880 to 1918, the next generation of technological innovation, which included the telegraph, telephone, wireless radio, and the airplane, led to new shifts in peoples’ perceptions of time and space, bringing a new round in “the leveling of traditional hierarchies” along with “a general cultural challenge to all outmoded hierarchies” (Kern, 1983, p. 315). But while these innovations eroded the old aristocracies and aided the rise of democracies, it was not long afterwards that new kinds of hierarchies emerged, from the awful totalitarian regimes of Adolph Hitler and Joseph Stalin, to the productive business corporations of Henry Ford, Pierre DuPont, and other capitalist innovators.

Today, the latest information revolution augurs not the end of hierarchy, but rather a new epoch of adaptation. Network designs may supplant hierarchical ones in some areas. In other areas, new kinds of hierarchies may emerge that are better suited to the information age. And in still other areas, synthetic hybrids of the two designs will be the result.

Adding a structural view to the processing view of information, as discussed earlier, clarifies that large-scale, purposeful, organizational change is a complex, dynamic, difficult undertaking. Organizations structure and process information; they are, or have at their core, systems for doing so.¹⁶ Change the organization, and those systems change with it. Tinker with those systems, and you may be tinkering, knowingly or unknowingly, with the organization's design and performance, for better or worse. For example, there is ample evidence by now that simply "throwing computers" at an organization often proves to be a misguided way to improve its efficiency and effectiveness. What, and how much, information (from any level of the "information pyramid") an organization can process well is bound to depend partly on what, and how much, information is already structurally embedded in it. Indeed, any form of organization—a hierarchy, a network, or whatever—may not work well until it embodies the values, norms, doctrines, rituals, etc. that are appropriate to that form.

Consider the four major forms that, over the ages, appear to account for the organization and evolution of societies: tribes, institutions, markets, and networks (see Ronfeldt, 1996). Very different types of information—and different information cultures and strategies—pertain to each form. In the case of tribes (and clans), the most valued information is often about kinship ties; in the case of institutions, it is about the reasons for hierarchy; in markets, it is about opportunities for exchange; and, while it is still early to be sure about information-age networks, information about the capacity for teamwork may be highly valued.

Thus, each of these forms depends on the existence of a different information culture, and on that culture being upheld through socialization and education, as well as law and punishment. Moreover, each form requires a different complexity of information structures and processes to function well—for example, from an informational

perspective, market systems are generally more complex than tribal systems. The appropriate design of technological infrastructures to support communication flows is only a part of the total picture of the ways in which information gets embedded in such systems—so deeply embedded that theorists and practitioners who are accustomed to looking more at transmitted than at embedded information may overlook how something that seems ordinary (e.g., routine marching drills, as noted earlier) may actually be a significant information agent.

Societies have spent centuries getting the hierarchical form right, all the time modifying it in accordance with new conditions. Getting the network form right in the future will be no easy task. Moreover, just as the organizational ecology of an advanced society like the United States is populated by various types of hierarchies, the future may lead to the emergence of various types of networks—and various ways of blending them with hierarchies. What emerges, and works, in one setting may not be the same in another.

At this point, a distinction should be made between the “organizational networks” and “networked organizations” that analysts have been writing about. The two are quite different. Although usage of the terms is not settled, we define an “organizational network” (or multiorganizational network) as consisting of a variety of actors who are often dispersed, who may belong to different independent organizations, and whose relationship is fundamentally nonhierarchical. A “networked organization” is a bounded organization (like a corporation) whose internal structure probably maintains a hierarchy at its core but that in other respects has evolved from a mainly hierarchical to a heavily networked design. Both types are subject to hybridization, the latter more so than the former. And both types figure in the hybrids we discuss next.

Hybrids of Hierarchies and Networks

Whoever masters the network form stands to gain major advantages in the coming epoch. For governments, this really means learning to develop hybrids.

Some hybrids already exist and are being tested. The business world is ahead of the government world in this respect. Modern corpora-

tions have spent the last few decades becoming “flatter,” and more networked. Large corporations still want to retain strong central control—but their production and marketing processes may well engage widespread networks of smaller companies. In the government world, signs of hybridization appear in efforts to build interagency and interservice networks. For example, counterterrorism and counternarcotics efforts involve mechanisms, some institutionalized and some ad-hoc, that aim to combine and coordinate mixes of military, police, and intelligence components. And some parts of the U.S. armed forces are also experimenting with networked designs, as noted in the next section. But none of the endeavors in the government and military worlds have yet provided sound models for forming hybrids of hierarchies and networks. One problem that continues to bedevil effective hybridization is that of overcoming (while also safeguarding) the participants’ institutional affiliations and loyalties to the hierarchies from which they come, while getting them to identify with and act in the interests of the interagency or interservice network.

While all this is being worked out, the destructive and disruptive powers of networks of small groups are gaining momentum all across the conflict spectrum. Thus, there is some urgency to learning to adapt and innovate around this factor. In the military area, for example, if the United States does not adjust to smaller units of maneuver, our large field armies, air wings, and naval battlegroups may face future difficulties grappling with nimble foes and may be quite vulnerable to their attacks. If we learn to rebuild around smaller (but stronger) military formations, the benefits may include providing for national security and military readiness at significantly reduced costs. In our view, the network, in particular the all-channel network, is the optimal form of organization for dealing with information-age conflict across the spectrum, from low to high intensity. However, this runs counter to much thinking in the defense community, where the attachment to hierarchical designs remains strong, and not without basis. Militaries, as many argue, must continue to have clear, top-down control, lest they founder under the “generalship of the many.” But the choice is not between shifting entirely to networks, or remaining entirely hierarchical. Rather, the key redesign questions revolve around the manner in which networks may be skillfully blended with hierarchies, so that, in Mao’s

famous phrase, one may “centralize strategically, but decentralize tactically.”

What might a hybrid look like in the U.S. military? The following scenario is speculative, but it is also consistent with the vision presented here: The chain of command is flattened, with many links removed that currently exist between the highest and lower levels. The highest levels of command are retained, including the regional commanders-in-chief (CINCs) and the National Command Authority (NCA). But the current structuring of forces into divisions and corps is replaced. New, small maneuver units are created as the backbone of the new structure, and their junior commanders have direct access to their CINCs (and vice versa). These units are roughly platoon-sized, and resemble the “infestation team” concept that the Marines are now experimenting with. These units are fully internettted; they are all able to communicate and coordinate with each other, independent of the higher command, although the CINC has awareness (topsite) of their communications and actions. Though headed by junior officers, the units can control and call on fire from assets “owned” by any service.

This is a radical scenario. It would surely be opposed by two- and three-star generals who currently command brigades, divisions and corps and thus stand between the CINCs and junior commanders of today’s maneuver units. But there is a historical wartime precedent for the scenario: Germany’s U-boat fleet during World War II. It had many of the characteristics noted above. Indeed, Admiral Dönitz, the U-boat campaign commander, made it a practice to meet as many returning U-boats as possible, often personally debriefing their junior-officer skippers (Dönitz, 1959). It is interesting to note that German submariners began to muse that they could do without the old, top-heavy hierarchy of the German military as early as World War I. But, near the end of that war, when Germany’s defeat seemed inevitable, the traditional, by-now-resentful, surface-fleet commanders called for creating a U-boat “cemetery” to put an end to this threat to their authority and their control of budgetary assets (Herwig, 1981).

This scenario calls for reductions in the levels of leadership above the field grade, but below the level of regional command. This might seem analogous to the frequent calls for the downsizing of “middle

management" in the business world in recent years. But this isn't quite what the scenario implies; it really targets the lower layer of upper management and views the junior commanders of the maneuver units as being more akin to middle-level managers.

The role of middle managers may turn out to be a key issue for the design of hybrid management systems. While all layers—from top to bottom—are affected by the information revolution, it is often said that middle management is the most affected—the flattening of hierarchies, in response to the information revolution, is widely supposed to spell the reduction if not elimination of many middle managers. Evidence exists for this by now, but it mainly involves middle managers who were performing information-processing and clerk-like functions. The story is not so clear where middle managers perform more innovative, operational functions. A few voices have noted this, keeping open the prospect that middle managers are far from obsolete, while more broadly defending the importance of hierarchy as an organizing principle: Layering remains entirely functional for the performance of complex tasks by large organizations, with about seven hierarchical layers being optimal (Jacques, 1990). Middle managers may be needed more than ever in the future, particularly to service and maintain links between different working groups in large organizations (Penzias, 1990). Ikujiro Nonaka and Hirotaka Takeuchi (1995) reach the farthest in not only praising middle managers for playing vital roles, but in urging that "middle up-down management" is often better than top-down or bottom-up designs for fostering knowledge creation in organizations. So, the debates about middle management's significance are far from settled (and depend partly on what layers are defined as "middle").

This aside, the foregoing scenario and the rest of our discussion indicate the likely essence of hybridization: Hierarchy is preserved, but flattening occurs, with the reductions coming from the lower-upper or the upper-middle command layers. Whether it is considered a facet of hierarchy or networking, the reformed structure allows, indeed requires, direct access and constant contact between the high-ranking commanders and the junior officers who head the maneuver units. The network design appears mainly in the all-channel links established among the maneuver units, and to the outside sources of intelligence and fire that they may call upon.

This is not a design that would work with any of today's military doctrines. It would require an entirely new doctrine.

TOWARD A DOCTRINE BASED ON SWARMING

We (not to mention our contributors) anticipate a landscape of conflict that calls not only for new organizational designs but also for related changes in doctrine. What operational behavior may be most effective for small, dispersed, mobile forces that are joined in networks? The short answer is swarming. Moving to smaller, dispersed units of maneuver may not bring advantages, and may make little sense, unless they have a deliberate, well-designed capability to swarm. If the optimal form of organization is the dispersed network, the corresponding doctrine must surely consist of the swarm.

Little analytic attention has been given to swarming (Kelly, 1994, is an exception). Yet, swarming may well become the key mode of conflict in the information age. New doctrines built around swarming are likely to emerge all across the conflict spectrum, for high- and low-intensity conflicts as well as for terrorist, criminal, and radical social conflicts. Indeed, swarming strategies are already emerging at the latter end of the spectrum.

Swarming is achieved when the dispersed nodes of a network of small (and also perhaps some large) forces can converge on an enemy from multiple directions, through either fire or maneuver. The overall aim should be sustainable pulsing—swarm networks must be able to coalesce rapidly and stealthily on a target, then disperse and redisperse, immediately ready to recombine for a new pulse. A swarm network should have little to no mass as a rule (except perhaps during a pulse), but it should have a high energy potential—like a swarm of bees that can fell a mighty beast, or a network of antibodies that can attack a spreading virus. The effect on an adversary is likely to be highly disruptive, and also highly destructive should the network wish to fire at will upon its disorganized foe. Today's trends toward tactical decentralization, coupled with strategic "top-sight" (the term is from Gelernter, 1991), may produce war-winning advantages as long as the new organization learns to fight in a new way.

Throughout history, organizational and technological innovations have affected the balance between the offense and defense. Some

innovations have initially favored the offense, others the defense. For example, the combination of tank and plane favored offensive blitzkrieg, whereas, a generation earlier, barbed wire and machine guns gave all the advantages to defensive trench warfare. At present, swarming is becoming more sustainable than ever for offensive operations, and more difficult to defend against. Thus, the development of a capacity for swarming, be that by a terrorist or a criminal organization, by a potential peer competitor, or by U.S. military and police forces, would probably favor whoever is determined to use swarming for offensive purposes.

Information and the Evolution of Organization and Doctrine

The correct conduct of all modes of conflict requires information—both structural information, so that people know (and are trained to know) what to do and why, in an organized manner, as well as information-processing systems, so they can spot attacks and targets, identify friend from foe, and coordinate operations. The history of warfare and other modes of conflict may be viewed, then, as a history of how organization and doctrine evolve depending on the information that can be embedded in and processed by them.

Beyond the foregoing examples, does the hypothesis about the co-evolution of information systems and battle doctrines fit the historical evidence more generally? Briefly, warfare has evolved from chaotic melees in which every man fought on his own, to the design of massed, but often rigid formations, and then to the adoption of maneuver. Each stage in this development is associated with a progression in the quantity and quality of information, from both structural and processing viewpoints. When there was little reason to train as a body, little ability to communicate during battle with one's own forces, and only notional understandings of the opponent's intentions, the free-for-all melee dominated. As means of signaling emerged (e.g., semaphores) and weaponry was introduced that benefited from coordinated fire (e.g., muskets), more controlled formations came into being (usually linear in nature). Further advances in organization and technology led to ever more supple maneuver capabilities, with mobile columns to some extent replacing linear formations (Van Creveld, 1985; Keegan, 1993). This progression in organization and doctrine—from the melee, to massing, to

maneuver—appears in all the realms of war: on land, at sea, and in the air.

While examples of this progression abound in each of the spatial domains of war, our points are neatly substantiated by the most modern of the three realms—air and space. Aerial operations, which arose this century, have followed a similar pattern, in which advances in combat formations have depended on information-related advances. In World War I, battles in the air by lone fighters were expressly “dogfights,” a kind of melee. Later, especially during World War II, the rise of the long-range bomber prompted the development of organized formations, with the spatial characteristics of air warfare militating against “lines” and favoring columns or “boxes” (e.g., the massed formations of B-17s). As for maneuver, air power’s close ties to advanced technologies, including for communications, have led it, from World War II onward, to move toward notions that resemble swarming, far more than has been the case with ground and naval power. This is evident in the fighter-bomber campaigns in France in 1944, Korea during 1950–1953, Vietnam from 1965 to 1973, and the Persian Gulf in 1991. Each of these swarm-like campaigns depended heavily upon massive, timely information flows for air tasking and battle management, as well as for the avoidance of fratricide (i.e., the bombing or strafing of one’s own troops). Indeed, without a sophisticated information-management capability, such as was afforded by JSTARS (the Joint Surveillance and Target Acquisition Radar System), the air campaign against Iraq in 1991 would have been only a fraction as effective as it proved to be (see Hallion, 1992).

The history of social conflict has been less comprehensively studied in terms of how organization and doctrine may be related to information; but it seems to contain a pattern much like that found in military history. Where groups of people are not well organized and have poor communications capabilities, riotous melees and shoving matches are often the main result. Likewise, the anarchism of violence-prone loners does not require much information from an organizational standpoint. The social equivalents of massing and maneuvering appear with the rise, in the 20th century, of Leninist parties and Maoist insurgencies. Modern-day terrorism aspires to blitzkrieg-like sophistication but rarely attains it.

Today, and on into the future, new information technologies enable the swarm. On the surface, it may bear some resemblance to the melee. But swarming is far more organized and requires expertly trained forces and the highest levels yet of command and control. The information revolution is the key to the development of new designs and capabilities for sustainable swarming—from the establishment of an initial posture of dispersed forces, to the coalescing of those forces for an attack, to their dissevering return to the safety of wide dispersion, and their preparation for a new pulse. Only a new generation of robust information gathering and distribution systems can support such pulsing.

History of Swarming As a Mode of Conflict

Before trying to look further into the future, we first want to clarify that swarming is not entirely new. It has occurred throughout history. Although it has not been, or been capable of becoming, a dominant approach to war and other modes of conflict until now, instructive historical examples exist of forces that maneuvered as networks and swarmed to the attack (or defense) as circumstances dictated.

A good example from medieval history is the Mongols' sweeping conquest of Asia on horseback (see Chapter Two). An excellent modern example of swarming at sea lies in the somewhat misnamed "wolf pack" tactics of the German U-boat fleet during World War II. These "wolves" did not run in a pack. Rather, they were distributed over a battlespace that, even at the tactical level (i.e., for a specific convoy battle), was spread over thousands of square kilometers. When a prime target set was located, telecommunications allowed the dispersed submarines to swarm upon the hapless convoy. This is the first case in naval history of a force whose maneuver units stayed quite far apart most of the time, then coalesced to swarm to the attack, and afterwards dissevered to return to scouting for new targets. As for swarming in the air, the Battle of Britain shows the use of radio and radar to enable the outnumbered fighters of the Royal Air Force to spot German air attacks and then swarm against them from a loose network of airfields distributed throughout central and southern England (Wood and Dempster, 1961; Deighton, 1977).

All these historical glimpses show that information is crucial to swarming, both to the coalescing of forces for the attack, and then to their dissevering return to the safety of wide dispersion. Only robust systems for gathering and distributing information can support such “pulsing” of combat forces.

This short review of doctrinal development suggests that the progression toward more complex, better organized and more effective fighting formations has gone hand in hand with advances in information management systems. In the case of air power in particular, there appears to be an emergent “swarming paradigm.” Will this hold true for land and naval warfare as well? Indeed, what may such a paradigm look like on land or at sea? For land campaigns, it may be necessary to look beyond current doctrine, even though it features integral air elements already. While the war against Saddam Hussein featured swarming air support for ground operations, the tank and mechanized divisions of Desert Storm massed, maneuvered, and fought in traditional fashion—much as they had trained to fight on the plains of Europe during the Cold War. It may be necessary for the Army to look beyond its own experiences and to consider the views emerging in other strategic cultures. The Chinese view of the impact of the information revolution on land warfare, as described in the introduction to this volume, may be a fruitful area to explore. In the information age, a variation on Mao’s doctrine of People’s War may prove more effective than the U.S. Army’s AirLand Battle doctrine. Continued American reliance upon massed, heavy mechanized forces may simply invite their destruction by precision weapons that, in the hands of skillful opponents, will themselves swarm the battlefield, as the French and Indians once did to General Braddock and his Redcoat regulars.

The Navy, whose air elements played no small part in the swarming air campaign in the Persian Gulf, has to think through a variety of issues, ranging from the future of the carrier to the potential of missile-laden “arsenal” ships. Of course, the very notion of a single ship armed with five hundred cruise missiles seems closely tied to the mentality of massing great firepower on as few platforms as possible. Other concerns relate to the ability of naval surface forces to cope with air and missile threats, and with the enduring problem of helping an amphibious force to land against a hostile shore. These are very big, complex issues, whose detailed resolution will require

decades of analysis and experimentation. Fortunately, there is no serious naval rival, giving the U.S. Navy the luxury of time to think these problems through carefully. Nevertheless, the organizational impulse to keep a large amount of firepower on a few large platforms should be seen as something of a violation of the principles of swarming. Because, although the cruise missiles fired from an arsenal ship might be able to swarm an attacker, the mother ship itself is a rich, inviting target for counterstrikes—much like the Japanese carriers that had massed closely at the Battle of Midway in 1942.

While the previous discussion emphasizes military history, swarming has also long figured in social conflicts. This is often evident in precursors to protest demonstrations, violent or nonviolent, where individuals and groups rapidly assemble, in a planned or spontaneous mass, and engage in a melee or march against an authority. Early examples of swarming arose during the social revolutions in Europe beginning in 1848, when urban citizens, sometimes joined by peasants from all over the countryside (and sometimes opposed by them), came together to fight governmental authorities in chaotic street-by-street melees.¹⁷ More recently, U.S. civil-rights and anti-Vietnam War groups in the 1960s and 1970s, some of which were linked as “segmented, polycentric, ideologically integrated networks” (SPINs),¹⁸ often held huge protest demonstrations that were partly the result of swarming by disparate groups, although many may have thought they were pursuing mainly a massing strategy.

Many past examples of swarming in social conflicts were more happenstance than deliberate. Today, a strong trend toward swarming is emerging, coming to the fore to supplant the earlier tendencies toward either riotous melees or mass marches. Perhaps the best recent example of “social swarming” is found in the response of the dozens of U.S., Canadian, and other activist NGOs whose representatives rushed, electronically as well as physically, into Mexico to pressure the Mexican government to deal with the 1994 Zapatista uprising through political negotiations rather than armed force. The result was that fighting died out after about two weeks and was followed by two years of energetic negotiations, while the NGOs worked to make sure that “information operations” continued to predominate over military operations.

Another recent example of social swarming is seen in the activities of the Serbian radio station B-92, which opposed the overturning of legitimate election results in 1996 by Slobodan Milosevic and gave voice to a rising political opposition movement. When the Serbian regime cut off its local broadcasting, the station's personnel put their programming on the Internet (using software called "RealAudio"). There it was picked up by the international media (including the Voice of America, the BBC, and Deutsche Welle), which not only proceeded to broadcast the programs back into Serbia, but also began pouring into Serbia to question the regime's behavior and cover pronouncements and demonstrations by the opposition movement. Thus, this case offers examples of both physical and virtual swarming.

Getting "BattleSwarm" Right

For swarming to be developed as a sound way to conduct conflict, new doctrines and related organizational designs, strategies, and tactics will have to be developed. Today, in the military area, advanced warfighting experiments (AWEs), such as Sea Dragon/Hunter Warrior in the Marines, and Force XXI/EXFOR in the Army, are under way that may generate innovations in this direction. None have a clear, precise focus on swarming; although the Marines' experimentation with small "infestation teams" is a significant step. More to the point, special operations forces have experimented with swarm-like tactics throughout history (Arquilla, 1996). Meanwhile, the major advances with swarming may be occurring at the other end of the conflict spectrum, among radical activists who want to use nonviolent "information operations" to put authoritarian regimes on the defensive, as in the case of the transnational activist NGOs who sided with the Zapatista movement in Mexico.

The term we would coin for referring to a well developed doctrine oriented to swarming is "BattleSwarm." By this, we mean a doctrine that could be applied across the full spectrum of conflict, from high to low intensity. At the high end, it would look beyond, and ultimately supersede, the current AirLand Battle doctrine. Just as Sun Tzu is said to be replacing Clausewitz as the key philosopher of war for the information age, so BattleSwarm may replace AirLand Battle as the optimal military doctrine. AirLand Battle refers to the close

cooperation of the Army and the Air Force in a blitzkrieg-like maneuver campaign in a high- or middle-intensity war. Unlike AirLand Battle, a BattleSwarm doctrine would involve all services in pulsing, oscillating, and, frequently, joint operations. BattleSwarm would also apply to conflicts at the low end of the spectrum, where it would guide nonmilitary as well as military operations against terrorist, guerrilla, and transnational criminal organizations.¹⁹

Achieving BattleSwarm would require the development of numerous new, relatively small, decentralized, team-like units of maneuver that are networked not only organizationally but also in terms of their access to command, control, communications, computers, and intelligence surveillance and reconnaissance (C4ISR) systems that enable the distribution of topsight. As noted earlier, the basic strategic, operational, and tactical aim would be to have a capability for sustainable pulsing, whereby the units can coalesce against a target, then disperse, redisperse, and be ready to recombine repeatedly until an adversary is defeated by disruption or destruction. In some situations, the dispersed units may join rapidly in a mass against a target; in other situations, they may remain dispersed while massing their fire in battle. Some situations may require high-precision stand-off strikes; others, close-in combat capabilities. Developing a BattleSwarm Doctrine and a set of forces to go with it would require unprecedented advances in information structuring and processing, not only so the maneuver teams could do what they are supposed to do under good circumstances, but also to ensure that they have robustness against electronic disruption.²⁰

AirLand Battle has strong proponents who would surely dispute our ideas about moving toward BattleSwarm. For example, Harry Summers (1995) argues that the "revolution in military affairs" has little substance, and that the old ways of AirLand Battle are tried and true. He believes that the United States actually needs a much bigger military to pursue the strategy of being able to win two major regional conflicts in close succession. From a similar perspective, Caspar Weinberger and Peter Schweizer (1997) maintain that, since winning the Cold War, the United States has gone back to having "hollow" armed forces that risk being caught short by the conflict scenarios that they envision. They, like Summers, recommend increases in military spending and prefer to expand on the ideals of AirLand Bat-

tle rather than to entertain radical doctrinal and organizational change.

Nonetheless, discussions about doctrinal change are well under way in the U.S. Army, where the leading views combine visions of dispersed deployment with notions of “convergent assault” (see Sullivan and Dubik, 1993; Coroalles, 1991; and Rothmann, 1991). While a step in the right direction, these views emphasize technology and, so far, have not extended to organizational redesign—they retain both the existing divisional structures, and the distinction between “heavy” (i.e., armored) and “light” divisions. Moreover, despite some interest in nonlinear operations, the main means of maneuver being envisioned is heliborne mobility. This does allow flexibility in unit movement; but helicopters are vulnerable to ground fire and are likely to remain so.

Heliborne mobility is likely to be an important aspect of deployment under a BattleSwarm doctrine—but not in the context of division-sized units of maneuver. Alexander (1995) sensibly urges a shift toward the adoption of much smaller, nimbler units of maneuver—a view that is in keeping with the emergence of BattleSwarm.

Another radical view is offered by the Friedmans (1997), who urge an equivalent of swarming in terms of the convergence of distant missile fires. Their approach would reduce the need for large field forces—but it does not seem suited to forcing a decision against an opponent that has dispersed his own forces, or deployed them in civilian population centers. A small, nimble opponent will be very hard to hit with distant missile fires from the United States or from American orbital platforms.

A BattleSwarm Scenario

One way to envision the likely contours of a BattleSwarm doctrine—in this case, one that may supersede AirLand Battle—is to sketch a scenario of a future conflict in which traditional approaches seem too costly, untimely, or uncertain as to the ultimate outcome. The Persian Gulf region continues to provide a good place for such a scenario since vital U.S. interests are unquestionably involved there, U.S. friends and allies are weak, the United States has few forces stationed in the region, and the strongest regional states (Iran and Iraq)

are unfriendly. Indeed, the region continues to be a subject of study, even as a likely catalyst for the outbreak of "strategic information warfare" (Molander, Riddile, and Wilson, 1996).

In the scenario we envision, assume that, ten years from now, the American policy of "dual containment" of Iran and Iraq has led to an entente between the two, aimed at diminishing U.S. influence in the region. Assume also that democratizing forces in Saudi Arabia are undermining the ruling regime, through a mix of violent acts as well as nonviolent "information operations" designed to uncover the foibles and misdeeds of King Fahd—a continuation and expansion of the current real-life campaign being waged by Mohammed al Masari against the Riyadh government. Finally, assume that some spark (e.g., a succession crisis after the passing of the king) ignites an internal conflict in Saudi Arabia in which the insurgents are supported by Iran, Iraq, and Yemen (the last of which also has very frosty relations with, and deep resentments against, the Saudi regime).

The externally supported rebels in Saudi Arabia quickly seize control of cities and ports, swarming over them in a few days and presenting the United States with a fait accompli. A provisional government of the new "Islamic Democratic Republic of Arabia" (IDRA) is swiftly recognized by Iran, Iraq, and Yemen (and by many other Islamic governments, notably Oman), who pledge military support. Many Islamic NGOs also declare their support for the new regime. Defensive preparations against an American counterintervention begin, with small detachments of Saudi rebels, Iranians, Iraqis, and Yemenis being stationed throughout the country. Further, the Iranians announce that they will close the Straits of Hormuz to any warships; the Yemenis make a similar pledge regarding passage to and through the southern approaches to the Red Sea. The field armies of the "big three" supporters of the revolution, which together total 100 divisions, are placed on alert, with roughly 12 divisions moved into the IDRA.

To cope with this catastrophe, let us assume that the United States strives first to cobble together an international consensus opposed to the new regime—but that it finds only lukewarm support in the U.N. and from its NATO allies. Russia and China threaten to use their vetoes to block U.N. authorization for use of force. At the same time, the small U.S. military contingents already in Saudi Arabia are ex-

pelled to Kuwait, which itself is now surrounded by hostile forces and isolated. Finally, American public opinion is confused, because the IDRA seems democratic and is offering continued oil sales at reduced prices. The Joint Chiefs tell the president that a U.S. intervention will require 750,000 troops, and casualties will be high. There is no friendly forward basing area, as the Omanis have not only refused permission for U.S. forces to deploy there, but, when asked to be accommodating, mobilize their own armed forces and call for help from the new IDRA government!

In short, the United States faces an apparently insuperable obstacle to restoring the Saudi ancien regime by forceful means. That is, it looks impossible to duplicate Desert Storm (or any other example of AirLand Battle). However, the president is persuaded that the U.S. military has been preparing itself for just such an impossible task. After convincing the American public that the “sovereignty” (and oil) of Saudi Arabia must be rescued, he (or she?) authorizes the Pentagon to unleash Operation “Desert Swarm.”

What follows is a campaign like none other in history. Two Marine divisions and the two Army divisions of the XVIII Airborne Corps (the 82nd and the 101st) redistribute their combat troops into roughly 100 company-sized (250 men) “task groups.” They are augmented by a similar number of small (6–8 man) Special Forces teams. All are linked electronically by a “SwarmNet,” allowing communications with each other and with the sea-based air and missile forces that will give them fire support. The Air Force is set to deliver strategic bombardment, with smart bombs and cruise missiles, as well as close air support for the ground maneuver units. Once lodgements on the Arabian peninsula are gained, forward air bases will be established for even more timely air support. A key element of the campaign is gaining the support of the heir apparent to King Fahd, who rallies his loyalists and calls for U.S. intervention.

The campaign that follows begins with many landings by U.S. forces on the long Red Sea coast of Saudi Arabia, after the Navy and Air Force quickly neutralize Yemeni patrol craft and missile bases at the southern approaches to the Red Sea, allowing fast landing and attack ships to transit this chokepoint. The Suez Canal is not used for initial landings but is employed for the movement of follow-on forces and supplies, since Israel and Egypt have declared their neutrality in the

conflict. Along with the heir apparent and his loyalists, U.S. forces help to liberate the holy places of Mecca and Medinah and engage Yemeni forces at numerous places in the south and Iraqis in several areas across the north. They have no idea how to grapple with the small American task groups, who are highly dispersed, able to maneuver, coalesce against a target, concentrate fire upon their opponents at will, and then disperse faster than the Yemenis (or any other forces) can respond. Since they cannot succeed on the offensive, they hole up in fortified areas. But these defenses are soon overcome by concentrated smart bombs and cruise missiles.

The Iranians, seeing that the Americans are not attempting to intervene via the Persian Gulf or Oman, attempt to send their four divisions to the western battle zone. But there is no fixed zone, no front, for their forces to focus on; and they are cut up by aerial bombing and special forces as they search for an enemy to engage. In a week, Desert Swarm's troops defeat the Islamic Alliance's regular forces, inspiring Saudis sympathetic to the heir apparent to rise up against IDRA and their foreign occupiers. The Alliance attempts to retreat, and is routed. Two weeks after the initial landings, the legitimate Saudi government is restored. American losses amount to 100 killed and 600 wounded. Twelve enemy divisions have been destroyed, and many others seriously damaged as they tried to engage the liberators. Thus, with fewer casualties, and by far fewer troops, Desert Swarm resulted in an even greater victory than the original Desert Storm.

After-action assessments conclude that the Saudi regime might well have been more permanently supplanted by IDRA if its leaders had waged a primarily nonviolent social netwar, attracting huge support from Islamic and Western activists, without involving Iranian or other outside military forces. Some U.S. intelligence analysts had warned of this possibility for several years, but they had been dismissed by their Saudi counterparts. Fortunately for U.S. interests, the radical Jihadist leadership behind IDRA had hubristic pretensions—while it presumed, correctly, that the United States would be unable to muster allies to replicate a Desert Storm, it took the further step of believing it could achieve a quicker, surer, and much sweeter seizure of power if it brandished arms and invited outside military support partly just to create an impossible, embarrassing situation for the United States. IDRA's leadership had no inkling (for that

matter, hardly anybody did) that the United States was capable of a Desert Swarm.

This scenario about the prospects for a BattleSwarm doctrine highlights the manner in which small, nimble, internettted forces might achieve great results against far more numerous opponents who subscribe to traditional doctrines. However, it is important to be mindful of the vulnerabilities of such a way of war before making any decisions to reshape U.S. forces radically. First, and foremost, all elements of a swarm must have robust communications capabilities; if the enemy can delink the task groups, which may be operating scores of miles apart, they might be attacked and defeated in detail. A swarm is made possible by information flows and is thus held at risk by their disruption. This means that the task groups must have “hardened” communications—and have plenty of spare radios—to cope with electromagnetic pulse as well as high-powered microwave weapons that might appear on the scene.

The foregoing suggests two necessary ingredients for moving toward a new doctrine with which to wage war in the information age: innovative organizational designs and a full appreciation that information flows are the ultimate logistical support required for combat operations.²¹ The military must network itself if it is to effect BattleSwarm. It must cut across service differences and distinctions, for a true swarm cannot exist where organizational loyalty to a service, branch, or combat specialty comes first. This organizational inter-netting must be held together, at the same time, by communications links never before approached in timeliness and comprehensiveness. Thus, even as organizational power diffuses down to quite small units, their ability to centralize fire upon targets may reach unparalleled heights of military effectiveness. This may be the essence of information-age military operations.

TOWARD A STRATEGY OF GUARDED OPENNESS

To function optimally, the organizational and doctrinal changes that we propose require unprecedented levels of information sharing. Such sharing is essential for the fulfillment of our vision. At the same time, this sharing must be protected, or secured, to prevent interference, surveillance, or predation by outsiders. For these reasons, this

strategic part of our vision revolves around the concept of “guarded openness,” a theme we raised in the preceding chapter.

In our view, guarded openness should be the guiding strategic principle that extends from the battlefield, to enable small units to network and swarm; through the level of grand strategy, where information is emerging as a distinct dimension, if not a new domain, of power. It should already be apparent from the organizational and doctrinal parts discussed above that swarm networks require robust systems for communications and information sharing. So, rather than amplify further on field-level concerns, we focus in this part on the grand strategic level.

We make three major points: First, “information” is reshaping the traditional political, economic, and military domains of grand strategy. Second, a distinct new domain of information strategy is emerging; and it may have its own dynamics, including its own subset of political, economic, and military concerns. Third, pursuing a strategy of guarded openness—a deliberately ambivalent pairing of words—will entail a constant balancing act, in which competing goals and concerns may be at stake, involving tensions and trade-offs between whether to stress openness or guardedness.

Basic Dynamics and Dimensions of Information Strategy

Information and communications have always been important to strategy. But now they are moving from being subsidiary concerns to becoming overarching ones. This is happening for reasons that did not exist even 20 years ago. One reason is the growth of a vast information infrastructure—notably the Internet, but also cable, direct broadcast satellites, cellular phones, etc.—in which the balance is shifting from one-to-many media (e.g., traditional radio and television broadcasting) to many-to-many media (e.g., the Internet and interactive Websites). A second reason, largely but not entirely a function of the first, is the huge increase in global interconnectivity, which is brought about by the ease of entry/access that exists in many nations, as well as by the growing, though varied, interests of so many parties in using the new infrastructure for commercial, social, diplomatic, military, and other interactions. A third reason is organizational: Vast arrays of nonstate interest groups are emerging that are explicitly concerned with information and communications

issues, such as the Electronic Freedom Foundation, and the Computer Professionals for Social Responsibility. These groups span the political spectrum and have diverse objectives that range from simply helping people get connected to the Net, to influencing government policies and laws, and advancing particular social causes at home or abroad.

Yet a fourth, mostly ideational, reason is a spreading recognition that information and power are increasingly linked. Across all political, economic, and military areas, we see the rise to primacy of informational “soft power” (see Nye and Owens, 1996), as opposed to the more traditional, material measures of power. This trend will require many years, probably a few decades, to unfold; and, in the interim, many traditional methods of exercising power may remain squarely at the center of conflict. But ultimately, the advent of “soft power” implies giving, sooner rather than later, a lot of innovative attention to the formulation of information strategy, since “power,” “security,” and “strategy” are increasingly up for redefinition.

In these and other respects, the advance of the information revolution over the last two decades has created a new strategic landscape that is replete with paradoxes and ambivalences. For example, war will likely be less bloody—but possibly much more disruptive to societies. The more advanced states may have greater technological capabilities—but also a richer set of targets for their “inferiors” to aim at. New nation-states are forming in many parts of the world—at the same time, power is diffusing rapidly to nonstate actors, often of an unruly variety. The rise of the network form heralds a new efficiency and effectiveness for all sorts of actors—but also poses the possibility that malefactors can start netwars (see Chapter Twelve) with low “entry costs” and sustain their efforts over long periods of time.

Some of these ambivalent and paradoxical dynamics go to a core concern for U.S. information strategy: Will the information revolution truly favor openness, or lead to new modes of political control? There is evidence that the new information technologies—especially the increased interconnectivity that comes with them—serve to open up closed systems. However, in some countries, the new technologies are creating incentives to reassert centralized control. For some government and corporate actors, the aim is to ensure social control

over people. But even where that is not the case, such actors may believe that they will not be able to maximize the benefits promised by interconnectivity unless they exert control over it.

The standard presumption is that power, particularly state power, goes hand in hand with control—in short, maximizing power means maximizing control. But this standard presumption is only partly correct. Power is sometimes optimized through harmonious decontrol. This may be the case, particularly over long time spans, when a major new system emerges that can best serve the overall functioning of a society if the system is left to operate according to its own rules and dynamics. A good example of this is the gradual rise of the market system in Europe during the 16th–18th centuries. The absolutist states of the times were accustomed to controlling commercial and other economic activities, and their inclinations to continue doing so, despite mounting control problems, gave rise to a period of mercantilism, before states realized that market systems would work better, and more to the benefit of home governments (including through the generation of tax revenues), if markets and business enterprises were left to their own dynamics. The growth of markets, and of the businesses that invigorated them, was greatly enabled by the electrical information revolution of the 19th and early 20th centuries (e.g., the telegraph, telephone, and wireless radio). Meanwhile, the domain of “economic strategy” came into being and developed separately from the domains of political and military strategy. More to the point, societies where state actors have learned to coexist and work with market actors—that is, where power extends as much from decontrol as from control—are today generally stronger and more influential than societies where states continue to dominate nascent market actors.

Today, the world appears to be on the threshold of another long-term systemic change, this time owing to the rise of the network form of organization, the attendant strengthening of civil-society and other nonstate actors, and the enabling effects of the digital information revolution. This systemic change, as much as anything, may turn out to be the catalyst for the emergence of information strategy as a distinct domain of grand strategy. But meanwhile, most (if not all) states are behaving as though the way to protect their power vis-à-vis this new generation of nonstate actors is to control them. In that sense, the dawning of the “age of networks” on the eve of the

21st century is mirroring a phenomenon that characterized the dawning of the “age of markets” in the 18th century: There is an increasing outcry for “freedom of information,” as there once was (and generally still is) for “freedom of trade.” But many states may prefer to try to prolong a period of strong control, a period of “information mercantilism” (not unlike the earlier period of economic mercantilism). Once again today, state power is being identified with control, even though the real, long-term benefits to the leading-edge states may ultimately accrue from letting a new network-based system “go” and learning to work with the civil-society actors who seem likely to form its core (Ronfeldt, 1996). In this interim period, some proclivities toward info-mercantilism may be unavoidable, and the development of information strategy will probably involve a curious interplay between the dynamics of control and decontrol.

How should the United States approach such an era? What might a strategy of “guarded openness” look like? If there is a single, overarching principle that should define the goals and principles of American information strategy, it should be a drive to foster openness. Politically, economically, and socially, the aim should be to encourage the creation and expansion of open, interconnected information systems. With regard to openness at the political and economic levels, we would urge a public diplomacy that serves to expand global interconnectivity, since this should not only help to foster the spread of free markets and open civil societies, but also pose political control problems for authoritarian regimes. The commendability of openness also applies in the military sphere; in the future, there will be a critical need for open lines of communications of all sorts—to one’s dispersed forces as well as to one’s allies. Indeed, the “freedom of the airwaves” may come, eventually, to replace the older strategic notion of the importance of the “freedom of the seas.”

But while openness should be the watchword of U.S. information strategy, there exist, on the guarded side of considerations, some serious risks to pursuing a uniform, across-the-board approach to openness. For example, in some international situations, it may be questionable to encourage political movements espousing free speech where they might spark the downfall of a friendly regime, such as the Fahd government in Saudi Arabia. Also, should diplomacy always strive for “open agreements, openly arrived at,” to use

Woodrow Wilson's phrase? Such openness characterized U.S. diplomacy during the early years of the recent Balkan War; but this gave Serb leaders the information that they needed—about the risk of U.S. intervention—to continue to pursue their expansionist, genocidal aims. Only when American policy turned a little more wily and unpredictable and began to include credible forceful options short of war, did the Serbs accept incentives to pursue a peaceful resolution to the conflict.

Furthermore, there are areas of great importance to national security where guardedness equates to protection, and openness may, in some situations, lead to unacceptable risks. In the military area, for example, governments and their militaries now depend on commercial off-the-shelf (COTS) products to enable and maintain their essential information infrastructures, in a world where there is little separation between national and global connectivity, and where COTS products are seldom under the control of single states. This reliance on COTS for military telecommunications, while providing a continuing means for obtaining the most advanced equipment at the lowest possible costs, may nevertheless engender risks of disruption, as potential adversaries will have an intimate understanding of their COTS-armed opponents' communications capabilities and vulnerabilities.

These examples highlight the point that democratic systems have generally aimed to strike a balance that promotes openness in principle, yet allows for guardedness in areas crucial to national security. But finding the right balance often proves elusive—and these few examples indicate that achieving the right mix between openness and guardedness will remain a nettlesome challenge.

Clearly, we believe that information strategy is emerging as a distinct domain, becoming more than just a modifier of the other elements of grand strategy. Similarly Alvin and Heidi Toffler (1993) discuss the rise of "knowledge strategy" as a new domain for "knowledge warriors." In their view (1993, p. 230), which we share,

Peace can sometimes be promoted by economic measures or imposed by force. But these are not the only available tools. Peace at the dawn of the twenty-first century requires the surgical application of a less tangible but frequently more potent weapon: knowledge.

However, neither we nor anyone else yet has a clear sense of what the boundaries of information strategy are, nor of precisely how information strategy differs from and compares in performance to the classic political, economic, and military domains of strategy. Can information strategies really help the United States to deal more effectively with its adversaries, open up closed societies, foster better relations with friends and allies, deter and manage conflicts abroad, and repel attacks on U.S. information assets?

To foster further thinking about this, we illuminate below one challenge likely to characterize the future—that of designing strategies to open up closed societies.²² We inquire as to how an informational approach may compare with, and improve upon, traditional approaches for dealing with a particular problem: Castro's Cuba.

An Illustrative Case: Opening a Closed Society

As a leading democracy, the United States has long made efforts to open up closed societies. It has generally done so by creating international political coalitions to upbraid dictatorships and by applying economic sanctions to pressure regimes to allow an opening of these societies. Military coercion has also been employed, both in the form of threats and actual interventions.

A prime example of the use of these traditional approaches is Cuba. Fidel Castro's regime has been the object of American political, economic, and military coercion for over 35 years, initially with the intent of isolating and toppling the regime, more recently with an emphasis on compelling the regime to liberalize. The United States has tried mightily to limit Cuba's diplomatic links, has maintained an economic embargo (recently trying to tighten it through the Helms-Burton legislation), and has even used military power to try to coerce changes in, or simply punish, the regime (e.g., the invasion of Cuban territory at the Bay of Pigs in 1961; the assault upon the Cuban detachment in Grenada in 1983; and other "strategic special operations").²³

None of these efforts has succeeded in toppling Castro's regime or compelling the liberalization of Cuba. Cuba has maintained extensive diplomatic relations with a multitude of countries throughout the period of U.S. efforts to achieve its political isolation. Economic

coercion efforts have been parried, first, by Cuba's having a "special" economic relationship with the Soviet Union, more recently by its cultivation of foreign investment, which has encouraged some countries to defy American policy. Furthermore, the Castro regime has retained the ability to convince the Cuban people to suffer hardships in response to American coercion. Finally, in the military realm, Cuban forces defeated the Bay of Pigs invasion; extracted a non-intervention pledge from the United States as part of the settlement of the 1962 Missile Crisis; and, from the mid-1970s through the early 1980s, engaged in a series of defiant military interventions in Africa.

The Cuban case does not represent a failure for U.S. strategy—in many ways, U.S. strategy has succeeded at containing and limiting the Castro regime. But U.S. strategy has not worked well in opening up this closed system. Does the case call out for the application of information strategy? Proposals have been fielded to that effect:

U.S. policies to isolate the Castro regime are well developed in the traditional areas of politics and economics. Meanwhile, technology advances are giving rise to a new area: information and communications policy. A lesson from the recent democratic revolutions in the East is that increased information and communications flows from the West, along with the adoption of related confidence-building measures in security areas, can penetrate and open up closed systems. Cuba may be ripe for application of this lesson. A comprehensive policy to open Cuba up could involve a range of steps, some of which may require modifying the embargo or other U.S. laws and restrictions (Gonzalez and Ronfeldt, 1992, p. 70).

What would an information strategy toward Cuba look like? Basically, it would aim at improving information flows into and out of the country, for reasons that include fostering the rise of civil society actors who would work to liberalize the country from within—in contrast to the traditional U.S. approach that emphasizes exerting pressures from the outside. For years, the United States waged an incipient information campaign built around Radio and TV Martí. But this is not enough. Among other initiatives, a broad-based information-age strategy might, for example, seek to provide Cubans with better connections to the Internet and better access to computer and network technologies. Such a strategy might also en-

courage Cubans to create NGOs concerned with information issues and communications rights.

In other contexts, such an informational approach has been treated as a possible general tool of U.S. foreign policy. The State Department has taken the position that “[t]he ability of people to communicate freely has long been recognized as a basic check on despotism” (United States Department of State, 1991, p. 2). In the 1980s, the Reagan Administration incorporated substantial informational elements into its foreign policy, as evinced by its support for the Solidarity movement in Poland and its direct pressure on the Soviet Union to open itself up. Indeed, the favorable Russian response, openness in the form of glasnost, unleashed social and political forces that the Kremlin simply could not control.

Could information strategy succeed in liberalizing Cuba where other elements of grand strategy have failed? Information strategy toward Cuba could hardly do worse than earlier approaches—and it may cost less and engender fewer political and military risks. Moreover, an American information strategy, depending on how it is shaped, might be viewed positively by the international community, a striking difference from the lack of international cooperation with current U.S. policy.

However, an information strategy toward Cuba may also face inherent, major limitations: the absence of independent NGOs and other elements of a full-fledged civil society; the presence of a strong state apparatus with many controls (including over the media); and the currently poor distribution of and limited access to communications technology, including Internet connections. For all these reasons, an information strategy toward Cuba may have to be treated as a long-term campaign, beginning with steps to improve Cuban information infrastructure, as well as to foster the rise of civil society. It might be best if the pursuit of these first, enabling steps of an information strategy could be led by transnational NGOs rather than by explicit U.S. government initiatives. But there again a limitation exists. Many NGOs are more sympathetic to Cuba’s plight than with U.S. policy.

As to the utility of information strategy, the Cuban case highlights the possibility that informational approaches may sometimes be com-

petitive with more coercive measures. For example, an effort to open Cuba up to the world might be contradicted by a continuing effort to strive for its political isolation, or to keep the economic embargo. To be sure, the information strategy against the old Soviet Union was coupled with continued political, economic, and military coercion (e.g., the American plan for a "Strategic Defense Initiative" posed a military threat that forced the Russians to spend more on defense at a time when their own economy was worsening). But the USSR was, in its time, a global power that jeopardized U.S. interests on every level for nearly half a century. This made it relatively easy to keep military pressure on the Soviet Union with one hand, while trying to open it up informationally with the other. Any notional Cuban "threat" pales by comparison. This implies that the United States can afford selectively easing military, economic, and diplomatic pressures against the Castro regime if that would help with the process of putting an effective information strategy in place. But any initiatives of these sorts should be considered warily. There is little reason to believe that easing up on such pressures would directly benefit either the few reformers inside the regime or the few dissidents who are pressing it from outside (Gonzalez, 1996). Moreover, we must recognize that Fidel Castro has long proven his own mastery of information strategy in his extended confrontation with the United States.

Broader Concerns About Opening up Closed Societies

Suppose we are not talking about just a single case, such as Cuba; but rather a range of cases around the world where informational approaches are attractive for inducing political, economic, and social liberalization. Then, we would be talking about engaging in a broad grand strategy of opening up closed societies—as is called for by the grand strategy known as "democratic enlargement." And, whether information strategy is pursued in conjunction with political, economic, and military initiatives, or on its own, it faces three general concerns that will inevitably arise: Is the strategy consistent, controllable, and ethical?

First, can one conceive of a consistent information strategy toward fostering open societies? If the hypothesis that increasing interconnectivity raises the price of repression is true, as seems the case, then

liberalizing effects should be generalized when such an approach is employed. But can information strategy be used so generally? Here it is important to consider the nature of the path to liberalization, which may include the serious social disruption of an authoritarian state. While this may seem desirable in the case of Cuba, it may pose unacceptably high risks in the case, say, of Saudi Arabia. Information might be used to bring down the regime of King Fahd; but this could also cause serious disruption in Saudi society, affecting vital oil flows, and possibly even aiding a successor government that is unfriendly toward the United States. Thus, pursuing a general information strategy of opening up closed societies must be viewed with caution—that is, “guardedly.”

A second concern relates to controllability—states are not able to control nonstate actors. The information revolution is empowering individuals and NGOs in ways that enable them to pursue their own strategies independent of state preferences. Some NGOs, notably ones that include expatriate dissidents, may even base themselves in an open society that is likely to defend their right to destabilize an authoritarian regime, even though it may be an ally of the state providing the launching point for the NGOs. Because information, and cyberspace, are transnational, or even supranational, the possibility exists that dissidents, physically located in one country, may exploit the Internet (or faxes, etc.) to undermine the political or social order in another country. In a recent example of this, the Britain-based Saudi Arabian expatriate, Mohammed al-Masari, mounted an Internet and fax campaign against the Fahd regime that led to strained Saudi-British relations.

A third concern is an ethical one. It flows from the paradox that supporting the desirable goal of opening up closed systems may entail fostering the outbreak of a great deal of social—and sometimes militarized—violence, with all the attendant consequences. In an ideal future, free speech should be protected as a public good and a personal right. However, the protection of all forms of free speech may create permissive conditions, notably for the waging of social networks designed to disrupt state stability and control. It is possible to argue that such disruption, if of a democratizing nature, is ultimately beneficial. However, there are difficulties and dilemmas, possibly moral as well as practical, that may be posed by the near-term disruption of friendly, even if authoritarian, states.

While this may be an inevitable cost of supporting freedom of speech, it may be prudent to search out ways to mitigate these societal costs. For example, a way to discourage the use of one state as a sanctuary for cyberspace political attacks upon another might exist if the “attacker” were an expatriate. Without undermining the principle of freedom of speech, the host government might communicate to the expatriate that the government could choose not to allow the expatriate to remain within its borders permanently. This control strategy might be attractive to states facing similar “hosting” dilemmas and might serve as a basis for an informal international cooperative regime. No doubt such a course of action would be fraught with legal complexity, highlighting just how difficult it will be to “secure” friends and allies from cyberspace activism, and how ripe the international system is for “social netwar” by nonstate actors in the information age.

These are but a few of the issues raised by the idea of developing information strategies to open up countries like Cuba, and to cope with the complications that may arise from seeing such strategies used to open up countries like Saudi Arabia. But the complications do not override a deeper point: Information strategy is likely to become a major domain and tool of statecraft in the decades ahead. It may well be that informational measures will eventually replace economic sanctions as the key tool of suasion in the information age, for two reasons. First, economic sanctions have just about run their course as an effective (some would say, ineffective) tool—it rarely works well. Second, information strategy should entail fewer costs, both to the innocent mass publics of the states being pressured, and to those countries who currently forgo trade with a target state as part of the economic war against it. If properly developed, information strategy may prove ethically, as well as practically, superior to the strategy of economic coercion.

Needed: An “RDA” to Match the RMA²⁴

Developing information strategy as a distinct domain will take a while. In the meantime, a host of information-age conflicts will likely arise, and means must be found to deter and prevent them when possible, and if not, then to manage them and achieve their termination. Conflict prevention, management, and resolution are principal

tasks of diplomacy. Diplomacy, though it has received little attention in this volume, normally plays crucial roles in the dramas of conflict prevention, management, and resolution. The challenges may be all the more complicated as information-age capabilities get mixed with the war-like, atavistic intentions that still haunt much of the world (Huntington, 1996; Kaplan, 1994). Diplomacy must not, therefore, be left out of any broad vision of information strategy.

It may be time to rethink diplomacy in terms of the themes elucidated in this volume—notably, the growing relationship between power and information, the rising utility of networked organizational designs, and the emergence of swarming capabilities. The United States has been undergoing a revolution in business affairs since the 1960s, and an RMA that began in the 1980s. Is it now time for a counterpart “revolution in diplomatic affairs” (an RDA)? A few voices have hinted at this (Cambone, 1996; Solomon, 1997; Nye and Owens, 1996; the U.S. Advisory Commission on Public Diplomacy, 1997). But for the most part, they have not yet been heard and heeded.

There are good reasons why the business and military worlds are in the throes of information-driven revolutions, and the diplomatic world is not. A key reason is that those worlds are driven by competition, in the first case between corporations, in the second between services. In addition, the business and military worlds are eager for technological enhancements. Also, the military suffered a major “defeat” in Vietnam that opened it up to innovative rethinking and redesign. None of this has been the case with the diplomatic world. The State Department has not been subject to much organizational competition. It has had little interest in technology and, like much of the government, has lagged in adopting it. Moreover, it has not suffered a defeat like Vietnam that would prompt radical innovation.

However, the diplomatic world is feeling some heat of competition now, especially from agile nonstate actors—both from those with which the State Department would like to cooperate, such as disaster-relief NGOs, and those that spell conflict, such as transnational terrorist and criminal organizations. Also, the State Department may be feeling a bit of competition vis-à-vis the military. The military and diplomatic communities have yet to master real-time, close-in cooperation (except in the case of the recent Dayton Accords)—and there

is a growing need for such cooperation. As the information age leads to new modes of conflict, there will be an increasing need to overcome compartmentalization and increase interagency, politico-military coordination. (Note the interplay between competition and cooperation here: The urge to compete is motivating—and it helps explain why and when a business, military, or diplomatic actor opts for innovation. But gaining a competitive edge depends not only on strengthening one's ability to compete against rivals and adversaries, but also on one's ability to cooperate with partners. One way to out-compete is to out-cooperate, a dynamic that is likely to be more important in the information age than in the industrial age as a result of the rise of the network form of organization.)

In another significant change for the diplomatic world, technologists are on the verge of producing tools that are as relevant for this world as they have been for the commercial and military worlds. Digital technology is now gaining momentum in such areas as: ubiquitous computing (with wireless, crypto, and handheld, low-cost devices everywhere); digital object infrastructures; intelligent agents; and tools for information visualization, including global networks of geographic information systems. Before long, video cameras will easily upload to the Internet; and satellite and other surveillance systems with high resolution will be widely available. At present, few diplomatic offices even have connectivity to the Internet; and few officers are even aware of technology developments that may prove useful to them. But interest is starting to grow in some diplomatic circles.

As the heat of competition and the allure of technology motivate diplomats to consider creating something like an RDA, they are becoming more aware that the information revolution is unsettling their world, often with the same ambivalent and paradoxical forces that the business and military worlds long ago recognized. Radical changes are now being recognized in the diplomatic world that mirror the changes that long ago aroused the business and military worlds. For example, there are rising tensions between the twin trends of, on one hand, an increasing centralization of control over diplomacy (within governments), and on the other hand, an increasing decentralization of control (due to the emergence of so many new nonstate actors). Moreover, like leaders in the business and military worlds, diplomats now increasingly complain that advanced telecommunications and other aspects of the information

revolution are altering the nature of diplomatic time and space: The information revolution is quickening the tempo of diplomacy, and forcing open its once-staid, largely closed processes. Ambassadors are finding that ever more actors involve themselves in a variety of issues—often in a public fashion—making it difficult for the ambassadors to speak as the sole authority. They have to engage more, and more diverse, actors early on. Their once orderly world is being roiled by the very same, deep dynamic that we have repeatedly called attention to: the dual shift in power (a) from large, hidebound actors to smaller, more agile ones, like NGOs; and (b) to actors, big or small, that can move away from stand-alone to networked forms of organization and behavior.

In short, there is now enough impetus in the world of diplomacy to propose that an RDA is plausible. Suppose it is: What would it look like? How might it unfold? First, it would have to heed a broad theme of this volume: Engaging in an information-based revolution is no simple matter; it is as much an organizational as a technological challenge and involves a broad rethinking of concepts, missions, doctrines, and strategies. Just hooking diplomats to the Internet and giving them cellular telephones might be small steps in the right direction; but this would not, in the overall scheme of things, do much to realize an RDA.

More to the point, an RDA would be well advised to heed a second, related theme of this volume: Whoever masters the network form stands to gain major advantages; for governments, this means coming up with hybrids of hierarchies and networks. One implication for the diplomatic world is to build networks to achieve a “deep coordination” between political and military officials, and between state and civil society actors. Building a range of collaborative networks between the public and private sectors, and between state and civil-society actors, would improve their mutual abilities to assess and address conflict-related issues. Both horizontal (e.g. interagency, and interstate) and vertical (e.g., state to nonstate) communications and coordination would have to be strengthened in the process, in efforts to resolve the tensions between centralization and decentralization.

In addition, an RDA should emphasize the establishment of numerous dispersed “nodes” that belong to the State Department. If so, it should cease its recent focus on closing consulates and refocus on

working to create more small consulates around the world.²⁵ This could help give the United States better knowledge for dealing with local conflicts. Despite all the talk that the information revolution spells “the end of territory” (because actors anywhere can now join together despite distance), local knowledge still matters greatly to diplomacy. Indeed, the next generation of technological tools, like geographic information systems, may well provide greater capabilities than ever for sharing local knowledge. As the “rise of geography” displaces the “end of territory” as a consequence of the information revolution, diplomats and other officials will surely see the importance of having small nodes dispersed worldwide as part of a vast array of “sensory organizations” made possible, perhaps imperative, by the information revolution (Ronfeldt, 1996).

Thus, for an RDA, like the RMA, the key challenge would be organizational. It has been said that the United States has developed a “works with” economy. An RDA implies developing a “works with” government—particularly one in which government actors increasingly engage nonstate actors in partnerships, including by building hybrid, just-in-time, virtual teams that can move quickly to address conflicts.²⁶ This poses the prospect that “information dominance” (Arquilla, 1994) may become as much a watchword for an RDA as for the RMA, and that information-sharing becomes the key to creating and exercising “soft power” (see Nye and Owens, 1996).

Who should take the initiative to foment an RDA? It should be the State Department. But if the State Department is not yet a ready environment for this, then institutions on its periphery may be better suited to providing the initiative—such institutions as the United States Information Agency, the Agency for International Development, and the United States Institute for Peace (which is sponsored by Congress).

* * * * *

It seems fitting to conclude this volume about how to prepare for conflict in the information age by emphasizing three insights that may help further the process of conflict limitation. First, while there will be much conflict in the future, it may well be more disruptive than destructive—making for far less bloodletting. This points to a hope that the 21st century will see the numbers of casualties drop to

a minuscule fraction of the 20th century's 100 million war dead. A second insight is that the era of massive armed forces is coming to an end—and with it the need for massive military expenditures. Perhaps we can all look forward to an “information dividend” that will prove far more real than the chimerical post-Cold War “peace dividend.” Finally, we see a possibility that informational resources and capabilities, judiciously employed, may actually prevent the outbreak of conflict. Our vision of a “revolution in diplomatic affairs” might thus be seen as a call for the rise of a global civil society devoted to “peace through wisdom”—an endeavor that would surely attract Athena's full support.

REFERENCES

- Alexander, Bevin, *The Future of Warfare*, New York: W. W. Norton, 1995.
- Allard, C. Kenneth, *Command, Control, and the Common Defense*, 2d edition, Washington, D.C.: National Defense University Press, 1997.
- Anderson, Benedict, *Imagined Communities: Reflections on the Origin and Spread of Nationalism*, Revised Edition, New York: Verso, 1991.
- Anderson, Perry, *Lineages of the Absolutist State*, London: Verso, 1974.
- Arquilla, John, “The Strategic Implications of Information Dominance,” *Strategic Review*, Summer 1994, pp. 24–30.
- , *From Troy to Entebbe: Special Operations in Ancient and Modern Times*, Lanham, Md.: University Press of America, 1996.
- Arquilla, John, and David Ronfeldt, “Cyberwar Is Coming!” *Comparative Strategy*, Vol. 12, No. 2, Summer 1993, pp. 141–165.
- , *The Advent of Netwar*, Santa Monica, Calif.: RAND, MR-789-OSD, 1996.
- Beniger, James R., *The Control Revolution: Technological and Economic Origins of the Information Society*, Cambridge, Mass.: Harvard University Press, 1986.

Bertalanffy, Ludwig von, *General System Theory: Foundations, Development, Applications*, Revised Edition, New York: George Braziller, 1968.

Bowker, Geoffrey, "Information Mythology: The World of/as Information," in Lisa Bud-Frierman, ed., *Information Acumen: The Understanding and Use of Knowledge in Modern Business*, New York: Routledge, 1994, pp. 231–247.

Bronowski, Jacob, *The Ascent of Man*, Boston, Mass.: Little, Brown and Co., 1973.

Cambone, Stephen A., *Kodak Moments, Inescapable Momentum, and the World Wide Web: Has the Infocomm Revolution Transformed Diplomacy?* McLean Va.: The Center for Information Strategy and Policy, Science Applications International Corporation, September 1996.

Capra, Fritjof, *The Web of Life: A New Scientific Understanding of Living Systems*, New York: Anchor Books, 1996.

Chalmers, David J., *The Conscious Mind: In Search of a Fundamental Theory*, New York: Oxford University Press, 1996.

Coroalles, Anthony M., "The Master Weapon: The Tactical Thought of J.F.C. Fuller Applied to Future War," *Military Review*, Vol. 71, January 1991, pp. 62–72.

Deighton, Len, *Fighter: The True Story of the Battle of Britain*, London: Jonathan Cape, 1977.

Dönitz, Karl von, *Memoirs: Ten Years and Twenty Days*, Cleveland: World Publishing Co., 1959 (reissued, Westport, Conn.: Greenwood Press, 1976).

Friedman, George and Meredith, *The Future of War*, New York: Crown, 1997.

Gelernter, David, *Mirror Worlds, or the Day Software Puts the Universe in a Shoebox . . . How It Will Happen and What It Will Mean*, New York: Oxford University Press, 1991.

Gerlach, Luther P., "Protest Movements and the Construction of Risk," in B. B. Johnson and V. T. Covello (eds.), *The Social and Cul-*

- tural Construction of Risk, Boston: D. Reidel Pub. Co., 1987, pp. 103–145.
- Gerlach, Luther P., and Virginia Hine, *People, Power, Change: Movements of Social Transformation*, New York: The Bobbs-Merrill Co., Inc., 1970.
- Gonzalez, Edward, *Cuba, Clearing Perilous Waters?* Santa Monica, Calif.: RAND, MR-673-OSD, 1996.
- Gonzalez, Edward, and David Ronfeldt, *Cuba Adrift in a Postcommunist World*, Santa Monica, Calif.: RAND, R-4231-USDP, 1992.
- Haefner, Klaus, ed., *Evolution of Information Processing Systems: An Interdisciplinary Approach to the Understanding of Nature and Society*, New York: Springer-Verlag, 1992.
- Haefner, Klaus, "Evolution of Information Processing—Basic Concept," in Haefner, ed., 1992, pp. 1–46.
- Hallion, David, *Storm over Iraq: Air Power and the Gulf War*, Washington, D.C.: Smithsonian Press, 1992.
- Harris, Marvin, *Cultural Materialism: The Struggle for a Science of Culture*, New York: Random House, 1979.
- Herwig, Holger, *Luxury Fleet*, Boston: Allen and Unwin, 1981.
- Hobsbawm, E. J., *The Age of Revolution: 1789–1848*, New York: New American Library, 1962.
- Huntington, Samuel P., *The Clash of Civilizations and the Remaking of World Order*, New York: Simon & Schuster, 1996.
- Jacques, Elliot, "In Praise of Hierarchy," *Harvard Business Review*, January–February 1990, pp. 127–133.
- Johnson, George, *Fire in the Mind: Science, Faith, and the Search for Order*, New York: Alfred A. Knopf, 1995.
- Kaplan, Robert, "The Coming Anarchy," *Atlantic Monthly*, February 1994, pp. 44–76.
- Keegan, John, *A History of Warfare*, New York: Vintage, 1993.

- Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization*, New York: Addison-Wesley Publishing Company, 1994.
- Kern, Stephen, *The Culture of Time and Space: 1880–1918*, Cambridge: Harvard University Press, 1983.
- Lenski, Gerhard, *Power and Privilege: A Theory of Social Stratification*, Chapel Hill: The University of North Carolina Press, 1966/1984.
- Marx, Karl, "The Defeat of June 1848," in Lewis S. Feuer, ed., *Marx and Engels: Basic Writings on Politics and Philosophy*, New York: Doubleday, [1850]1959, pp. 281–307.
- McNeill, William H., *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000*, Chicago: The University of Chicago Press, 1982.
- Melody, William, "Electronic Networks, Social Relations, and the Changing Structure of Knowledge," in David Crowley and David Mitchell, eds., *Communication Theory Today*, Stanford: Stanford University Press, 1994, pp. 254–273.
- Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica, Calif.: RAND, MR-661-OSD, 1996.
- Nonaka, Ikujiro, and Hirotaka Takeuchi, *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, New York: Oxford University Press, 1995.
- Nye, Joseph S., and William A. Owens, "America's Information Edge," *Foreign Affairs*, March/April 1996, pp. 20–36.
- Oeser, Erhard, "From Neural Information Processing to Knowledge Technology," in Haefner, ed., 1992, pp. 320–340.
- Penzias, Arno, *Information and Ideas: Managing in a High-Tech World*, New York: Simon & Schuster Inc., 1990.
- Rogers, Everett M., *A History of Communications Studies: A Biographical Approach*, New York: The Free Press, 1994.

- Ronfeldt, David, "Cyberocracy Is Coming," *The Information Society*, Vol. 8, No. 4, 1992, pp. 243-296.
- , *Tribes, Institutions, Markets, Networks: A Framework About Societal Evolution*, Santa Monica, Calif.: RAND, P-7967, 1996.
- Rosen, Stephen Peter, *Winning the Next War: Innovation and the Modern Military*, Ithaca: Cornell University Press, 1991.
- Roszak, Theodore, *The Cult of Information: The Folklore of Computers and the True Art of Thinking*, New York: Pantheon Books, 1986.
- Rothmann, Harry E., "The U.S. Army, Strategic Formulation, and Force Planning," Newport, R.I.: Naval War College, 1991.
- Simon, Herbert A., "The Architecture of Complexity," *Proceedings of the American Philosophical Society*, No. 106, December 1962, pp. 467-482 (reprinted in Herbert A. Simon, *The Sciences of the Artificial*, Second Edition, Cambridge: The MIT Press, 1981, pp. 193-229).
- Skocpol, Theda, *States and Social Revolutions: A Comparative Analysis of France, Russia, and China*, New York: Cambridge University Press, 1979.
- Solomon, Richard H., *The Global Information Revolution and International Conflict Management*, Address to the conference on "Virtual Diplomacy," Washington, D.C.: United States Institute for Peace, April 1997.
- Sullivan, General Gordon L., and James Dubik, *Land Warfare in the 21st Century*, Carlisle, Pa.: Army War College, 1993.
- Summers, Harry, *The New World Strategy*, New York: Simon and Schuster, 1995.
- Toffler, Alvin, and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-first Century*, Boston: Little, Brown and Company, 1993.
- Tufte, Edward R., *The Visual Display of Quantitative Information*, Cheshire, Conn.: Graphics Press, 1983.

-----, *Envisioning Information*, Cheshire, Conn.: Graphics Press, 1990.

United States Advisory Commission on Public Diplomacy, *A New Diplomacy for the Information Age*, Washington, D.C.: United States Advisory Commission on Public Diplomacy, 1997.

United States Department of State, Bureau of International Communications and Information Policy, Washington, D.C.: U.S. Department of State, Publication 9860, 1991.

Van Creveld, Martin, *Command in War*, Cambridge: Harvard, 1985.

-----, "In Wake of Terrorism, Modern Armies Prove to Be Dinosaurs of Defense," *New Perspectives Quarterly*, Vol. 13, No. 4, Fall 1996, pp. 57-58.

Vandenbroucke, Lucien S., *Perilous Options: Special Operations As an Instrument of U.S. Foreign Policy*, London: Oxford University Press, 1993.

Waltz, Kenneth, *Theory of International Politics*, New York: McGraw-Hill, 1979.

Weinberger, Caspar, and Peter Schweizer, *The Next War*, Chicago: Regnery, 1997.

Wood, Derek, and Derek Dempster, *The Narrow Margin: The Battle of Britain and the Rise of Air Power*, London: Hutchinson, 1961.

Wright, Robert, *Three Scientists and Their Gods: Looking for Meaning in an Age of Information*, New York: Harper & Row, 1989.

NOTES

¹In a somewhat wry paper, historian Geoffrey Bowker (1994) observes that, over the ages, the more information has seemed central to the world's economic processes, the more it has affected peoples' views of time and space, and the more it has come to be viewed as a key organizing principle of the universe, finally giving rise to expansive philosophical and scientific claims that "everything is information."

²Johnson (1995, pp. 110-111) writes: "Most of us are used to thinking of information as secondary, not fundamental, something that is made from matter and energy. Whether we are thinking of petroglyphs carved in a cliff or the electromagnetic waves beaming from transmitters on Sandia Crest, information seems like an artifact, a human invention. We impose pattern on matter and energy and use it to signal our

fellow humans. Though information is used to describe the universe, it is not commonly thought of as being part of the universe itself. But to many of those at the Santa Fe conference, the world just didn't make sense unless information was admitted into the pantheon, on an equal footing with mass and energy. A few went so far as to argue that information may be the most fundamental of all; that mass and energy could somehow be derived from information."

³For example, Bertalanffy (1968, p. 27), using the term "function" to cover process, writes, "In the last resort, structure (i.e., order of parts) and function (order of processes) may be the very same thing: in the physical world, matter dissolves into a play of energies, and in the biological world structures are the expression of a flow of processes." Waltz (1979, p. 40), using the term "interaction" instead of process, writes, "A system is then defined as a set of interacting units. At one level, a system consists of a structure, and the structure is the systems-level component that makes it possible to think of the units as forming a set instead of a mere collection. At another level, the system consists of interacting units. . . . Any approach or theory, if it is rightly termed 'systemic,' must show how the system's level, or structure, is distinct from the level of interacting units."

⁴For example, according to Skocpol (1979, p. 4), "Social revolutions are rapid, basic transformations of a society's state and class structures Social revolutions are set apart from other sorts of conflicts and transformative processes above all by the combinations of two coincidences: the coincidence of societal structural change with class upheaval; and the coincidence of political with social transformation. . . . Political revolutions transform state structures but not social structures, and they are not necessarily accomplished through class conflict. And processes such as industrialization can transform social structures without necessarily bringing about, or resulting from, sudden political upheavals or basic political-structural changes."

⁵For example, according to Lenski, (1966, p. 43), "In analyses of social stratification, it is a temptation to turn immediately to the interesting and much debated structural problems, such as those concerning the nature, number, and composition of classes. While such questions must inevitably be a part of any adequate treatment of the subject, they are secondary in importance to questions about the processes which give rise to the structures. Moreover, to attempt to deal with the structural problems without prior attention to these processes, as is sometimes done, is to put the cart before the horse and create confusion."

⁶Cognitive scientist David Chalmers (1996) makes an intriguing attempt to treat information as the link between the physical and phenomenal worlds that may be required to arrive at a theory of consciousness. He relies on the "it from bit" kind of theoretical physics (e.g., by Edward Fredkin) that figures in Wright's book.

⁷Much the same may occur with visual displays—graphics—of quantitative information. As Tufte (1983, p. 191) writes, "What is to be sought in designs for the display of information is the clear portrayal of complexity. Not the complication of the simple; rather the task of the designer is to give visual access to the subtle and the difficult—that is, the revelation of the complex." Tufte (1990, p. 51) adds, "What about confusing clutter? Information overload? Doesn't data have to be 'boiled down' and 'simplified'? These common questions miss the point, for the quantity of data is an issue completely separate from the difficulty of reading. Clutter and confusion are failures of design, not attributes of information."

⁸Actually, we still have a lot of literature to consult, including by philosophers who talk about "practices" and "disclosive spaces" and "clearings" (our thanks to Peter Denning for pointing this out).

⁹Roszak (1986, p. 90) defines "ideas" as "integrating patterns" and associates them with knowledge. Building up a structural view to balance the processing view may provide a way to ease the concerns of harsh critics, like Roszak.

¹⁰Recognizing this, Xerox has announced a research effort, supported by its Palo Alto Research Center (PARC), to design computerized tools and methods to discriminate "tacit knowledge" from run-of-the-mill information in corporate settings. The success of this effort could spell a major advance toward establishing a knowledge processing capability.

¹¹The terms "structure" and "infrastructure" are quite common. The term "superstructure" and its identification with ideational structures comes from Karl Marx, in connection with his argument that the nature of a society's "base"—its mode of production—determines the nature of its superstructure. Building on Marx, Harris's (1979) anthropological theory of cultural materialism re-terms this base as the infrastructure and distinguishes it from a society's structure and superstructure. His use of terms is the closest we have found to our own. However, our use of the term infrastructure is more technological than his, in keeping with the term's usage today to refer to local, national, and global information infrastructures. We do not subscribe to the proposition that the infrastructure largely determines the superstructure. Laws and related rules and regulations are sometimes treated as an infrastructure.

¹²Studies about business and market systems often view laws and regulations as belonging to the "legal infrastructure" of those systems. In noting this, we recognize that there are other approaches than the one we pose here for us to consider as we seek to further develop and refine our framework. In the present framework, we are viewing law in a very broad sense. We would include, by the way, laws about freedom of assembly and association and about rights to communication and information—these may have particular bearing on a people's ability to establish local NGOs and connect to the Internet.

¹³Libraries and the print media might be included here as well.

¹⁴We may find, in future efforts to confirm and elaborate on this framework, that the information-processing view has its own ideational, organizational, technological, and even linguistic layers. If so, this could help with building a framework that bridges the structural and processing views.

¹⁵These points are consistent with another point: Around the world, in places as diverse as Canada, China, Iran, and France, people knowledgeable about the information revolution evince some concerns about the vulnerabilities of their information and communications infrastructures to destructive attacks, but they are equally, if not considerably more, concerned about how the presence of the Internet and other advanced telecommunications infrastructures may expose their cultures to erosion. They may worry about a particular process (Americanization), but their ultimate fear is more structural (the risks to their identity and sovereignty).

¹⁶Much the same may be said for societies as a whole. Melody (1994) provides a structure-oriented statement about this, and Beniger (1986) a process-oriented statement.

¹⁷The causes and patterns of defeat of these violent social swarms are analyzed by Marx ([1850]1959, pp. 281–307). Hobsbawm (1962, p. 361) observes that there was, nevertheless, a sense of promise in 1848: “An entire continent waited, ready by now to pass the news of revolution almost instantly from city to city by means of the electric telegraph” (emphasis added).

¹⁸We discuss SPINs in Arquilla and Ronfeldt (1996). The SPIN concept, first identified by anthropologist Luther Gerlach and sociologist Virginia Hine (Gerlach, 1987; Gerlach & Hine, 1970), refers to the following characteristics that they found in U.S. social movements in the 1960s and 1970s: “By segmentary I mean that it is cellular, composed of many different groups By polycentric I mean that it has many different leaders or centers of direction By networked I mean that the segments and the leaders are integrated into reticulated systems or networks through various structural, personal, and ideological ties. Networks are usually unbounded and expanding This acronym [SPIN] helps us picture this organization as a fluid, dynamic, expanding one, spinning out into mainstream society” (Gerlach, 1987, p. 115).

¹⁹More to the point, the doctrine we elucidate here might just as easily be redrawn and developed from the viewpoints of a terrorist, criminal, or other adversarial organization at the low end of the conflict spectrum. Some U.S. militia groups have already moved in this direction, notably those that subscribe to the doctrine known as “leaderless resistance” espoused by Aryan nationalist Louis Beam (see Arquilla and Ronfeldt, 1996).

²⁰Allard (1997) provides solid, practical advice about how to restructure information flows to optimize military performance.

²¹As for regular logistics, a suggestion has cropped up in one briefing we have seen that it should move toward a concept of “swarm logistics” in the future.

²²This is but one type of scenario that may be used to illuminate information strategy. We hope to explore others in future writings. These scenarios might reflect challenges such as working with allies, defending the United States from a broad-based information attack (one that is perceptual as well as technological), and enhancing our ability to cope with a burgeoning politico-military crisis.

²³Vandenbroucke (1993) details the many coercive military efforts mounted against the Castro regime, focusing principally on the Bay of Pigs invasion.

²⁴The ideas in this section are based largely on the attendance by one of the authors at the conference on “Virtual Diplomacy: The Global Communications Revolution and International Conflict Management,” organized by the U.S. Institute for Peace, Washington, D.C., April 1–2, 1997.

²⁵This point about consulates was made by former Secretary of State George Shultz at the conference on “Virtual Diplomacy” in April 1997 (see footnote immediately above).

²⁶Canada’s Foreign Ministry has reportedly moved much farther in this direction than has the U.S. State Department.